|  |  |  |  |
| --- | --- | --- | --- |
|  | A picture containing screenshot, font, graphics, logo  Description automatically generated | Controlled Unclassified Information info@fedramp.gov  fedramp.gov |  |

|  |  |  |
| --- | --- | --- |
|  | A blue and white logo  Description automatically generated with medium confidence |  |

FedRAMP® System Security Plan (SSP)  
Appendix A: High FedRAMP Security Controls

**for Microsoft**

**Azure Commercial**

Version 1.0

9/15/2024

Appendix A High Azure Commercial FedRAMP Security Controls

The definitions in Table A-1. Control Origination and Definitions indicate where each security control originates.

| **Control Origination** | **Definition** | **Example** |
| --- | --- | --- |
| **Service Provider Corporate** | A control that originates from a CSP’s corporate network. | DNS from the corporate network provides address resolution services for the information system and the service offering. |
| **Service Provider System Specific** | A control specific to a particular CSP system and the control is not part of the standard corporate controls. | A unique host-based intrusion detection system (HIDs) is available on the service offering platform, but is not available on the corporate network. |
| **Service Provider Hybrid** | A control that makes use of both corporate controls and additional controls specific to a particular CSP system. | There are scans of the corporate network infrastructure; scans of databases and Web-based applications are system specific. |
| **Configured by Customer** | A control where a customer needs to apply a configuration to meet the control requirement. | User profiles, policy/audit configurations, enabling/disabling key switches (e.g., enable/disable http\* or https, etc.), entering an IP range specific to their organization are configurable by the customer. |
| **Provided by Customer** | A control where a customer needs to provide additional hardware or software to meet the control requirement. | A customer provides a SAML SSO solution to implement two-factor authentication. |
| **Shared** | A control that is managed and implemented partially by a CSP and partially by their customer. | Security awareness training must be conducted by both the CSPN and a CSP’s customer. |
| **Inherited from pre-existing FedRAMP Authorization** | A control that is inherited from another CSP system that has already received a FedRAMP authorization. | A PaaS or SaaS provider inherits PE controls from an IaaS provider. |

Table of Contents

[Access Control (AC) 17](#_Toc176967883)

[AC-1 Policy and Procedures 17](#_Toc176967884)

[AC-2 Account Management 22](#_Toc176967885)

[AC-2(1) - Automated System Account Management 37](#_Toc176967886)

[AC-2(2) - Automated Temporary and Emergency Account Management 39](#_Toc176967887)

[AC-2(3) - Disable Accounts 40](#_Toc176967888)

[AC-2(4) - Automated Audit Actions 42](#_Toc176967889)

[AC-2(5) - Inactivity Logout 44](#_Toc176967890)

[AC-2(7) - Privileged User Accounts 45](#_Toc176967891)

[AC-2(9) - Restrictions on Use of Shared and Group Accounts 49](#_Toc176967892)

[AC-2(11) - Usage Conditions 50](#_Toc176967893)

[AC-2(12) - Account Monitoring for Atypical Usage 51](#_Toc176967894)

[AC-2(13) - Disable Accounts for High-risk Individuals 53](#_Toc176967895)

[AC-3 Access Enforcement 55](#_Toc176967896)

[AC-4 Information Flow Enforcement 57](#_Toc176967897)

[AC-4(4) - Flow Control of Encrypted Information 60](#_Toc176967898)

[AC-4(21) - Physical or Logical Separation of Information Flows 62](#_Toc176967899)

[AC-5 Separation of Duties 64](#_Toc176967900)

[AC-6 Least Privilege 67](#_Toc176967901)

[AC-6(1) - Authorize Access to Security Functions 68](#_Toc176967902)

[AC-6(2) - Non-privileged Access for Nonsecurity Functions 70](#_Toc176967903)

[AC-6(3) - Network Access to Privileged Commands 72](#_Toc176967904)

[AC-6(5) - Privileged Accounts 73](#_Toc176967905)

[AC-6(7) - Review of User Privileges 74](#_Toc176967906)

[AC-6(8) - Privilege Levels for Code Execution 76](#_Toc176967907)

[AC-6(9) - Log Use of Privileged Functions 77](#_Toc176967908)

[AC-6(10) - Prohibit Non-privileged Users from Executing Privileged Functions 79](#_Toc176967909)

[AC-7 Unsuccessful Logon Attempts 80](#_Toc176967910)

[AC-8 System Use Notification 82](#_Toc176967911)

[AC-10 Concurrent Session Control 86](#_Toc176967912)

[AC-11 Device Lock 88](#_Toc176967913)

[AC-11(1) - Pattern-hiding Displays 90](#_Toc176967914)

[AC-12 Session Termination 91](#_Toc176967915)

[AC-14 Permitted Actions Without Identification or Authentication 93](#_Toc176967916)

[AC-17 Remote Access 95](#_Toc176967917)

[AC-17(1) - Monitoring and Control 98](#_Toc176967918)

[AC-17(2) - Protection of Confidentiality and Integrity Using Encryption 99](#_Toc176967919)

[AC-17(3) - Managed Access Control Points 101](#_Toc176967920)

[AC-17(4) - Privileged Commands and Access 102](#_Toc176967921)

[AC-18 Wireless Access 105](#_Toc176967922)

[AC-18(1) - Authentication and Encryption 107](#_Toc176967923)

[AC-18(3) - Disable Wireless Networking 108](#_Toc176967924)

[AC-18(4) - Restrict Configurations by Users 109](#_Toc176967925)

[AC-18(5) - Antennas and Transmission Power Levels 111](#_Toc176967926)

[AC-19 Access Control for Mobile Devices 112](#_Toc176967927)

[AC-19(5) - Full Device or Container-based Encryption 114](#_Toc176967928)

[AC-20 Use of External Systems 115](#_Toc176967929)

[AC-20(1) - Limits on Authorized Use 117](#_Toc176967930)

[AC-20(2) - Portable Storage Devices - Restricted Use 119](#_Toc176967931)

[AC-21 Information Sharing 120](#_Toc176967932)

[AC-22 Publicly Accessible Content 122](#_Toc176967933)

[Awareness and Training (AT) 125](#_Toc176967934)

[AT-1 Policy and Procedures 125](#_Toc176967935)

[AT-2 Literacy Training and Awareness 130](#_Toc176967936)

[AT-2(2) - Insider Threat 133](#_Toc176967937)

[AT-2(3) - Social Engineering and Mining 134](#_Toc176967938)

[AT-3 Role-based Training 136](#_Toc176967939)

[AT-4 Training Records 138](#_Toc176967940)

[Audit and Accountability (AU) 140](#_Toc176967941)

[AU-1 Policy and Procedures 140](#_Toc176967942)

[AU-2 Event Logging 145](#_Toc176967943)

[AU-3 Content of Audit Records 150](#_Toc176967944)

[AU-3(1) - Additional Audit Information 152](#_Toc176967945)

[AU-4 Audit Log Storage Capacity 154](#_Toc176967946)

[AU-5 Response to Audit Logging Process Failures 156](#_Toc176967947)

[AU-5(1) - Storage Capacity Warning 158](#_Toc176967948)

[AU-5(2) - Real-time Alerts 159](#_Toc176967949)

[AU-6 Audit Record Review, Analysis, and Reporting 161](#_Toc176967950)

[AU-6(1) - Automated Process Integration 165](#_Toc176967951)

[AU-6(3) - Correlate Audit Record Repositories 166](#_Toc176967952)

[AU-6(4) - Central Review and Analysis 168](#_Toc176967953)

[AU-6(5) - Integrated Analysis of Audit Records 169](#_Toc176967954)

[AU-6(6) - Correlation with Physical Monitoring 171](#_Toc176967955)

[AU-6(7) - Permitted Actions 172](#_Toc176967956)

[AU-7 Audit Record Reduction and Report Generation 174](#_Toc176967957)

[AU-7(1) - Automatic Processing 176](#_Toc176967958)

[AU-8 Time Stamps 177](#_Toc176967959)

[AU-9 Protection of Audit Information 179](#_Toc176967960)

[AU-9(2) - Store on Separate Physical Systems or Components 181](#_Toc176967961)

[AU-9(3) - Cryptographic Protection 183](#_Toc176967962)

[AU-9(4) - Access by Subset of Privileged Users 184](#_Toc176967963)

[AU-10 Non-repudiation 186](#_Toc176967964)

[AU-11 Audit Record Retention 188](#_Toc176967965)

[AU-12 Audit Record Generation 190](#_Toc176967966)

[AU-12(1) - System-wide and Time-correlated Audit Trail 192](#_Toc176967967)

[AU-12(3) - Changes by Authorized Individuals 193](#_Toc176967968)

[Assessment, Authorization, and Monitoring (CA) 195](#_Toc176967969)

[CA-1 Policy and Procedures 195](#_Toc176967970)

[CA-2 Control Assessments 200](#_Toc176967971)

[CA-2(1) - Independent Assessors 205](#_Toc176967972)

[CA-2(2) - Specialized Assessments 206](#_Toc176967973)

[CA-2(3) - Leveraging Results from External Organizations 208](#_Toc176967974)

[CA-3 Information Exchange 210](#_Toc176967975)

[CA-3(6) - Transfer Authorizations 212](#_Toc176967976)

[CA-5 Plan of Action and Milestones 214](#_Toc176967977)

[CA-6 Authorization 216](#_Toc176967978)

[CA-7 Continuous Monitoring 220](#_Toc176967979)

[CA-7(1) - Independent Assessment 225](#_Toc176967980)

[CA-7(4) - Risk Monitoring 226](#_Toc176967981)

[CA-8 Penetration Testing 228](#_Toc176967982)

[CA-8(1) - Independent Penetration Testing Agent or Team 230](#_Toc176967983)

[CA-8(2) - Red Team Exercises 232](#_Toc176967984)

[CA-9 Internal System Connections 233](#_Toc176967985)

[Configuration Management (CM) 236](#_Toc176967986)

[CM-1 Policy and Procedures 236](#_Toc176967987)

[CM-2 Baseline Configuration 242](#_Toc176967988)

[CM-2(2) - Automation Support for Accuracy and Currency 248](#_Toc176967989)

[CM-2(3) - Retention of Previous Configurations 250](#_Toc176967990)

[CM-2(7) - Configure Systems and Components for High-risk Areas 251](#_Toc176967991)

[CM-3 Configuration Change Control 253](#_Toc176967992)

[CM-3(1) - Automated Documentation, Notification, and Prohibition of Changes 259](#_Toc176967993)

[CM-3(2) - Testing, Validation, and Documentation of Changes 263](#_Toc176967994)

[CM-3(4) - Security and Privacy Representatives 264](#_Toc176967995)

[CM-3(6) - Cryptography Management 266](#_Toc176967996)

[CM-4 Impact Analyses 268](#_Toc176967997)

[CM-4(1) - Separate Test Environments 270](#_Toc176967998)

[CM-4(2) - Verification of Controls 272](#_Toc176967999)

[CM-5 Access Restrictions for Change 273](#_Toc176968000)

[CM-5(1) - Automated Access Enforcement and Audit Records 275](#_Toc176968001)

[CM-5(5) - Privilege Limitation for Production and Operation 277](#_Toc176968002)

[CM-6 Configuration Settings 279](#_Toc176968003)

[CM-6(1) - Automated Management, Application, and Verification 285](#_Toc176968004)

[CM-6(2) - Respond to Unauthorized Changes 287](#_Toc176968005)

[CM-7 Least Functionality 289](#_Toc176968006)

[CM-7(1) - Periodic Review 292](#_Toc176968007)

[CM-7(2) - Prevent Program Execution 294](#_Toc176968008)

[CM-7(5) - Authorized Software - Allow-by-exception 295](#_Toc176968009)

[CM-8 System Component Inventory 298](#_Toc176968010)

[CM-8(1) - Updates During Installation and Removal 302](#_Toc176968011)

[CM-8(2) - Automated Maintenance 303](#_Toc176968012)

[CM-8(3) - Automated Unauthorized Component Detection 305](#_Toc176968013)

[CM-8(4) - Accountability Information 308](#_Toc176968014)

[CM-9 Configuration Management Plan 309](#_Toc176968015)

[CM-10 Software Usage Restrictions 312](#_Toc176968016)

[CM-11 User-installed Software 315](#_Toc176968017)

[CM-12 Information Location 318](#_Toc176968018)

[CM-12(1) - Automated Tools to Support Information Location 321](#_Toc176968019)

[CM-14 Signed Components 323](#_Toc176968020)

[Contingency Planning (CP) 324](#_Toc176968021)

[CP-1 Policy and Procedures 324](#_Toc176968022)

[CP-2 Contingency Plan 330](#_Toc176968023)

[CP-2(1) - Coordinate with Related Plans 336](#_Toc176968024)

[CP-2(2) - Capacity Planning 337](#_Toc176968025)

[CP-2(3) - Resume Mission and Business Functions 339](#_Toc176968026)

[CP-2(5) - Continue Mission and Business Functions 340](#_Toc176968027)

[CP-2(8) - Identify Critical Assets 341](#_Toc176968028)

[CP-3 Contingency Training 343](#_Toc176968029)

[CP-3(1) - Simulated Events 345](#_Toc176968030)

[CP-4 Contingency Plan Testing 347](#_Toc176968031)

[CP-4(1) - Coordinate with Related Plans 349](#_Toc176968032)

[CP-4(2) - Alternate Processing Site 351](#_Toc176968033)

[CP-6 Alternate Storage Site 353](#_Toc176968034)

[CP-6(1) - Separation from Primary Site 354](#_Toc176968035)

[CP-6(2) - Recovery Time and Recovery Point Objectives 356](#_Toc176968036)

[CP-6(3) - Accessibility 357](#_Toc176968037)

[CP-7 Alternate Processing Site 358](#_Toc176968038)

[CP-7(1) - Separation from Primary Site 361](#_Toc176968039)

[CP-7(2) - Accessibility 363](#_Toc176968040)

[CP-7(3) - Priority of Service 364](#_Toc176968041)

[CP-7(4) - Preparation for Use 366](#_Toc176968042)

[CP-8 Telecommunications Services 367](#_Toc176968043)

[CP-8(1) - Priority of Service Provisions 369](#_Toc176968044)

[CP-8(2) - Single Points of Failure 370](#_Toc176968045)

[CP-8(3) - Separation of Primary and Alternate Providers 372](#_Toc176968046)

[CP-8(4) - Provider Contingency Plan 373](#_Toc176968047)

[CP-9 System Backup 375](#_Toc176968048)

[CP-9(1) - Testing for Reliability and Integrity 380](#_Toc176968049)

[CP-9(2) - Test Restoration Using Sampling 381](#_Toc176968050)

[CP-9(3) - Separate Storage for Critical Information 382](#_Toc176968051)

[CP-9(5) - Transfer to Alternate Storage Site 384](#_Toc176968052)

[CP-9(8) - Cryptographic Protection 386](#_Toc176968053)

[CP-10 System Recovery and Reconstitution 387](#_Toc176968054)

[CP-10(2) - Transaction Recovery 389](#_Toc176968055)

[CP-10(4) - Restore Within Time Period 391](#_Toc176968056)

[Identification and Authentication (IA) 393](#_Toc176968057)

[IA-1 Policy and Procedures 393](#_Toc176968058)

[IA-2 Identification and Authentication (Organizational Users) 398](#_Toc176968059)

[IA-2(1) - Multi-factor Authentication to Privileged Accounts 400](#_Toc176968060)

[IA-2(2) - Multi-factor Authentication to Non-privileged Accounts 401](#_Toc176968061)

[IA-2(5) - Individual Authentication with Group Authentication 402](#_Toc176968062)

[IA-2(6) - Access to Accounts -separate Device 404](#_Toc176968063)

[IA-2(8) - Access to Accounts - Replay Resistant 406](#_Toc176968064)

[IA-2(12) - Acceptance of PIV Credentials 407](#_Toc176968065)

[IA-3 Device Identification and Authentication 409](#_Toc176968066)

[IA-4 Identifier Management 411](#_Toc176968067)

[IA-4(4) - Identify User Status 415](#_Toc176968068)

[IA-5 Authenticator Management 416](#_Toc176968069)

[IA-5(1) - Password-based Authentication 422](#_Toc176968070)

[IA-5(2) - Public Key-based Authentication 427](#_Toc176968071)

[IA-5(6) - Protection of Authenticators 430](#_Toc176968072)

[IA-5(7) - No Embedded Unencrypted Static Authenticators 433](#_Toc176968073)

[IA-5(8) - Multiple System Accounts 434](#_Toc176968074)

[IA-5(13) - Expiration of Cached Authenticators 436](#_Toc176968075)

[IA-6 Authentication Feedback 437](#_Toc176968076)

[IA-7 Cryptographic Module Authentication 439](#_Toc176968077)

[IA-8 Identification and Authentication (Non-organizational Users) 444](#_Toc176968078)

[IA-8(1) - Acceptance of PIV Credentials from Other Agencies 445](#_Toc176968079)

[IA-8(2) - Acceptance of External Authenticators 447](#_Toc176968080)

[IA-8(4) - Use of Defined Profiles 448](#_Toc176968081)

[IA-11 Re-authentication 449](#_Toc176968082)

[IA-12 Identity Proofing 451](#_Toc176968083)

[IA-12(2) - Identity Evidence 454](#_Toc176968084)

[IA-12(3) - Identity Evidence Validation and Verification 456](#_Toc176968085)

[IA-12(4) - In-person Validation and Verification 457](#_Toc176968086)

[IA-12(5) - Address Confirmation 459](#_Toc176968087)

[Incident Response (IR) 461](#_Toc176968088)

[IR-1 Policy and Procedures 461](#_Toc176968089)

[IR-2 Incident Response Training 466](#_Toc176968090)

[IR-2(1) - Simulated Events 469](#_Toc176968091)

[IR-2(2) - Automated Training Environments 471](#_Toc176968092)

[IR-3 Incident Response Testing 473](#_Toc176968093)

[IR-3(2) - Coordination with Related Plans 475](#_Toc176968094)

[IR-4 Incident Handling 476](#_Toc176968095)

[IR-4(1) - Automated Incident Handling Processes 481](#_Toc176968096)

[IR-4(2) - Dynamic Reconfiguration 482](#_Toc176968097)

[IR-4(4) - Information Correlation 484](#_Toc176968098)

[IR-4(6) - Insider Threats 485](#_Toc176968099)

[IR-4(11) - Integrated Incident Response Team 486](#_Toc176968100)

[IR-5 Incident Monitoring 488](#_Toc176968101)

[IR-5(1) - Automated Tracking, Data Collection, and Analysis 489](#_Toc176968102)

[IR-6 Incident Reporting 491](#_Toc176968103)

[IR-6(1) - Automated Reporting 494](#_Toc176968104)

[IR-6(3) - Supply Chain Coordination 495](#_Toc176968105)

[IR-7 Incident Response Assistance 497](#_Toc176968106)

[IR-7(1) - Automation Support for Availability of Information and Support 499](#_Toc176968107)

[IR-8 Incident Response Plan 501](#_Toc176968108)

[IR-9 Information Spillage Response 506](#_Toc176968109)

[IR-9(2) - Training 510](#_Toc176968110)

[IR-9(3) - Post-spill Operations 511](#_Toc176968111)

[IR-9(4) - Exposure to Unauthorized Personnel 512](#_Toc176968112)

[Maintenance (MA) 514](#_Toc176968113)

[MA-1 Policy and Procedures 514](#_Toc176968114)

[MA-2 Controlled Maintenance 519](#_Toc176968115)

[MA-2(2) - Automated Maintenance Activities 524](#_Toc176968116)

[MA-3 Maintenance Tools 526](#_Toc176968117)

[MA-3(1) - Inspect Tools 529](#_Toc176968118)

[MA-3(2) - Inspect Media 530](#_Toc176968119)

[MA-3(3) - Prevent Unauthorized Removal 532](#_Toc176968120)

[MA-4 Nonlocal Maintenance 534](#_Toc176968121)

[MA-4(3) - Comparable Security and Sanitization 537](#_Toc176968122)

[MA-5 Maintenance Personnel 539](#_Toc176968123)

[MA-5(1) - Individuals Without Appropriate Access 541](#_Toc176968124)

[MA-6 Timely Maintenance 543](#_Toc176968125)

[Media Protection (MP) 545](#_Toc176968126)

[MP-1 Policy and Procedures 545](#_Toc176968127)

[MP-2 Media Access 549](#_Toc176968128)

[MP-3 Media Marking 551](#_Toc176968129)

[MP-4 Media Storage 553](#_Toc176968130)

[MP-5 Media Transport 555](#_Toc176968131)

[MP-6 Media Sanitization 558](#_Toc176968132)

[MP-6(1) - Review, Approve, Track, Document, and Verify 560](#_Toc176968133)

[MP-6(2) - Equipment Testing 562](#_Toc176968134)

[MP-6(3) - Nondestructive Techniques 563](#_Toc176968135)

[MP-7 Media Use 565](#_Toc176968136)

[Physical and Environmental Protection (PE) 567](#_Toc176968137)

[PE-1 Policy and Procedures 567](#_Toc176968138)

[PE-2 Physical Access Authorizations 572](#_Toc176968139)

[PE-3 Physical Access Control 575](#_Toc176968140)

[PE-3(1) - System Access 582](#_Toc176968141)

[PE-4 Access Control for Transmission 583](#_Toc176968142)

[PE-5 Access Control for Output Devices 585](#_Toc176968143)

[PE-6 Monitoring Physical Access 586](#_Toc176968144)

[PE-6(1) - Intrusion Alarms and Surveillance Equipment 589](#_Toc176968145)

[PE-6(4) - Monitoring Physical Access to Systems 590](#_Toc176968146)

[PE-8 Visitor Access Records 592](#_Toc176968147)

[PE-8(1) - Automated Records Maintenance and Review 595](#_Toc176968148)

[PE-9 Power Equipment and Cabling 596](#_Toc176968149)

[PE-10 Emergency Shutoff 598](#_Toc176968150)

[PE-11 Emergency Power 600](#_Toc176968151)

[PE-11(1) - Alternate Power Supply - Minimal Operational Capability 601](#_Toc176968152)

[PE-12 Emergency Lighting 603](#_Toc176968153)

[PE-13 Fire Protection 604](#_Toc176968154)

[PE-13(1) - Detection Systems - Automatic Activation and Notification 606](#_Toc176968155)

[PE-13(2) - Suppression Systems - Automatic Activation and Notification 607](#_Toc176968156)

[PE-14 Environmental Controls 609](#_Toc176968157)

[PE-14(2) - Monitoring with Alarms and Notifications 611](#_Toc176968158)

[PE-15 Water Damage Protection 613](#_Toc176968159)

[PE-15(1) - Automation Support 614](#_Toc176968160)

[PE-16 Delivery and Removal 615](#_Toc176968161)

[PE-17 Alternate Work Site 617](#_Toc176968162)

[PE-18 Location of System Components 620](#_Toc176968163)

[Planning (PL) 621](#_Toc176968164)

[PL-1 Policy and Procedures 621](#_Toc176968165)

[PL-2 System Security and Privacy Plans 626](#_Toc176968166)

[PL-4 Rules of Behavior 631](#_Toc176968167)

[PL-4(1) - Social Media and External Site/Application Usage Restrictions 635](#_Toc176968168)

[PL-8 Security and Privacy Architectures 636](#_Toc176968169)

[PL-10 Baseline Selection 640](#_Toc176968170)

[PL-11 Baseline Tailoring 641](#_Toc176968171)

[Personnel Security (PS) 643](#_Toc176968172)

[PS-1 Policy and Procedures 643](#_Toc176968173)

[PS-2 Position Risk Designation 647](#_Toc176968174)

[PS-3 Personnel Screening 649](#_Toc176968175)

[PS-3(3) - Information Requiring Special Protective Measures 652](#_Toc176968176)

[PS-4 Personnel Termination 654](#_Toc176968177)

[PS-4(2) - Automated Actions 657](#_Toc176968178)

[PS-5 Personnel Transfer 659](#_Toc176968179)

[PS-6 Access Agreements 662](#_Toc176968180)

[PS-7 External Personnel Security 665](#_Toc176968181)

[PS-8 Personnel Sanctions 668](#_Toc176968182)

[PS-9 Position Descriptions 671](#_Toc176968183)

[Risk Assessment (RA) 673](#_Toc176968184)

[RA-1 Policy and Procedures 673](#_Toc176968185)

[RA-2 Security Categorization 678](#_Toc176968186)

[RA-3 Risk Assessment 681](#_Toc176968187)

[RA-3(1) - Supply Chain Risk Assessment 686](#_Toc176968188)

[RA-5 Vulnerability Monitoring and Scanning 690](#_Toc176968189)

[RA-5(2) - Update Vulnerabilities to Be Scanned 697](#_Toc176968190)

[RA-5(3) - Breadth and Depth of Coverage 698](#_Toc176968191)

[RA-5(4) - Discoverable Information 700](#_Toc176968192)

[RA-5(5) - Privileged Access 701](#_Toc176968193)

[RA-5(8) - Review Historic Audit Logs 702](#_Toc176968194)

[RA-5(11) - Public Disclosure Program 704](#_Toc176968195)

[RA-7 Risk Response 706](#_Toc176968196)

[RA-9 Criticality Analysis 707](#_Toc176968197)

[System and Services Acquisition (SA) 709](#_Toc176968198)

[SA-1 Policy and Procedures 709](#_Toc176968199)

[SA-2 Allocation of Resources 714](#_Toc176968200)

[SA-3 System Development Life Cycle 717](#_Toc176968201)

[SA-4 Acquisition Process 722](#_Toc176968202)

[SA-4(1) - Functional Properties of Controls 730](#_Toc176968203)

[SA-4(2) - Design and Implementation Information for Controls 731](#_Toc176968204)

[SA-4(5) - System, Component, and Service Configurations 733](#_Toc176968205)

[SA-4(9) - Functions, Ports, Protocols, and Services in Use 735](#_Toc176968206)

[SA-4(10) - Use of Approved PIV Products 736](#_Toc176968207)

[SA-5 System Documentation 737](#_Toc176968208)

[SA-8 Security and Privacy Engineering Principles 743](#_Toc176968209)

[SA-9 External System Services 745](#_Toc176968210)

[SA-9(1) - Risk Assessments and Organizational Approvals 748](#_Toc176968211)

[SA-9(2) - Identification of Functions, Ports, Protocols, and Services 750](#_Toc176968212)

[SA-9(5) - Processing, Storage, and Service Location 751](#_Toc176968213)

[SA-10 Developer Configuration Management 753](#_Toc176968214)

[SA-11 Developer Testing and Evaluation 756](#_Toc176968215)

[SA-11(1) - Static Code Analysis 759](#_Toc176968216)

[SA-11(2) - Threat Modeling and Vulnerability Analyses 761](#_Toc176968217)

[SA-15 Development Process, Standards, and Tools 763](#_Toc176968218)

[SA-15(3) - Criticality Analysis 766](#_Toc176968219)

[SA-16 Developer-provided Training 767](#_Toc176968220)

[SA-17 Developer Security and Privacy Architecture and Design 769](#_Toc176968221)

[SA-21 Developer Screening 772](#_Toc176968222)

[SA-22 Unsupported System Components 774](#_Toc176968223)

[System and Communications Protection (SC) 776](#_Toc176968224)

[SC-1 Policy and Procedures 776](#_Toc176968225)

[SC-2 Separation of System and User Functionality 781](#_Toc176968226)

[SC-3 Security Function Isolation 783](#_Toc176968227)

[SC-4 Information in Shared System Resources 785](#_Toc176968228)

[SC-5 Denial-of-service Protection 787](#_Toc176968229)

[SC-7 Boundary Protection 790](#_Toc176968230)

[SC-7(3) - Access Points 799](#_Toc176968231)

[SC-7(4) - External Telecommunications Services 800](#_Toc176968232)

[SC-7(5) - Deny by Default - Allow by Exception 805](#_Toc176968233)

[SC-7(7) - Split Tunneling for Remote Devices 807](#_Toc176968234)

[SC-7(8) - Route Traffic to Authenticated Proxy Servers 809](#_Toc176968235)

[SC-7(10) - Prevent Exfiltration 810](#_Toc176968236)

[SC-7(12) - Host-based Protection 812](#_Toc176968237)

[SC-7(18) - Fail Secure 814](#_Toc176968238)

[SC-7(20) - Dynamic Isolation and Segregation 815](#_Toc176968239)

[SC-7(21) - Isolation of System Components 817](#_Toc176968240)

[SC-8 Transmission Confidentiality and Integrity 818](#_Toc176968241)

[SC-8(1) - Cryptographic Protection 822](#_Toc176968242)

[SC-10 Network Disconnect 824](#_Toc176968243)

[SC-12 Cryptographic Key Establishment and Management 826](#_Toc176968244)

[SC-12(1) - Availability 836](#_Toc176968245)

[SC-13 Cryptographic Protection 837](#_Toc176968246)

[SC-15 Collaborative Computing Devices and Applications 847](#_Toc176968247)

[SC-17 Public Key Infrastructure Certificates 849](#_Toc176968248)

[SC-18 Mobile Code 851](#_Toc176968249)

[SC-20 Secure Name/Address Resolution Service (Authoritative Source) 853](#_Toc176968250)

[SC-21 Secure Name/Address Resolution Service (Recursive or Caching Resolver) 856](#_Toc176968251)

[SC-22 Architecture and Provisioning for Name/Address Resolution Service 858](#_Toc176968252)

[SC-23 Session Authenticity 860](#_Toc176968253)

[SC-24 Fail in Known State 862](#_Toc176968254)

[SC-28 Protection of Information at Rest 863](#_Toc176968255)

[SC-28(1) - Cryptographic Protection 866](#_Toc176968256)

[SC-39 Process Isolation 868](#_Toc176968257)

[SC-45 System Time Synchronization 869](#_Toc176968258)

[SC-45(1) - Synchronization with Authoritative Time Source 871](#_Toc176968259)

[System and Information Integrity (SI) 873](#_Toc176968260)

[SI-1 Policy and Procedures 873](#_Toc176968261)

[SI-2 Flaw Remediation 878](#_Toc176968262)

[SI-2(2) - Automated Flaw Remediation Status 884](#_Toc176968263)

[SI-2(3) - Time to Remediate Flaws and Benchmarks for Corrective Actions 885](#_Toc176968264)

[SI-3 Malicious Code Protection 887](#_Toc176968265)

[SI-4 System Monitoring 893](#_Toc176968266)

[SI-4(1) - System-wide Intrusion Detection System 899](#_Toc176968267)

[SI-4(2) - Automated Tools and Mechanisms for Real-time Analysis 900](#_Toc176968268)

[SI-4(4) - Inbound and Outbound Communications Traffic 902](#_Toc176968269)

[SI-4(5) - System-generated Alerts 905](#_Toc176968270)

[SI-4(10) - Visibility of Encrypted Communications 906](#_Toc176968271)

[SI-4(11) - Analyze Communications Traffic Anomalies 908](#_Toc176968272)

[SI-4(12) - Automated Organization-generated Alerts 910](#_Toc176968273)

[SI-4(14) - Wireless Intrusion Detection 912](#_Toc176968274)

[SI-4(16) - Correlate Monitoring Information 913](#_Toc176968275)

[SI-4(18) - Analyze Traffic and Covert Exfiltration 914](#_Toc176968276)

[SI-4(19) - Risk for Individuals 916](#_Toc176968277)

[SI-4(20) - Privileged Users 918](#_Toc176968278)

[SI-4(22) - Unauthorized Network Services 919](#_Toc176968279)

[SI-4(23) - Host-based Devices 921](#_Toc176968280)

[SI-5 Security Alerts, Advisories, and Directives 923](#_Toc176968281)

[SI-5(1) - Automated Alerts and Advisories 927](#_Toc176968282)

[SI-6 Security and Privacy Function Verification 929](#_Toc176968283)

[SI-7 Software, Firmware, and Information Integrity 932](#_Toc176968284)

[SI-7(1) - Integrity Checks 937](#_Toc176968285)

[SI-7(2) - Automated Notifications of Integrity Violations 940](#_Toc176968286)

[SI-7(5) - Automated Response to Integrity Violations 942](#_Toc176968287)

[SI-7(7) - Integration of Detection and Response 944](#_Toc176968288)

[SI-7(15) - Code Authentication 946](#_Toc176968289)

[SI-8 Spam Protection 948](#_Toc176968290)

[SI-8(2) - Automatic Updates 950](#_Toc176968291)

[SI-10 Information Input Validation 951](#_Toc176968292)

[SI-11 Error Handling 953](#_Toc176968293)

[SI-12 Information Management and Retention 955](#_Toc176968294)

[SI-16 Memory Protection 957](#_Toc176968295)

[Supply Chain Risk Management (SR) 958](#_Toc176968296)

[SR-1 Policy and Procedures 958](#_Toc176968297)

[SR-2 Supply Chain Risk Management Plan 963](#_Toc176968298)

[SR-2(1) - Establish SCRM Team 966](#_Toc176968299)

[SR-3 Supply Chain Controls and Processes 967](#_Toc176968300)

[SR-5 Acquisition Strategies, Tools, and Methods 972](#_Toc176968301)

[SR-6 Supplier Assessments and Reviews 976](#_Toc176968302)

[SR-8 Notification Agreements 979](#_Toc176968303)

[SR-9 Tamper Resistance and Detection 981](#_Toc176968304)

[SR-9(1) - Multiple Stages of System Development Life Cycle 982](#_Toc176968305)

[SR-10 Inspection of Systems or Components 983](#_Toc176968306)

[SR-11 Component Authenticity 984](#_Toc176968307)

[SR-11(1) - Anti-counterfeit Training 988](#_Toc176968308)

[SR-11(2) - Configuration Control for Component Service and Repair 989](#_Toc176968309)

[SR-12 Component Disposal 991](#_Toc176968310)

# Access Control (AC)

## AC-1 Policy and Procedures

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (OneOrMore): organization-level;mission/business process-level;system-level] access control policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the access control policy and the associated access controls;

b. Designate an [an official to manage the access control policy and procedures is defined;] to manage the development, documentation, and dissemination of the access control policy and procedures; and

c. Review and update the current access control:

1. Policy [at least annually] and following [events that would require the current access control policy to be reviewed and updated are defined;] ; and

2. Procedures [at least annually] and following [significant changes].

|  |
| --- |
| **AC-1 Control Summary Information** |
| Responsible Roles: SOP Team, Policy |
| Parameter ac-1(a): all personnel |
| Parameter ac-01\_odp.01: |
| Parameter ac-01\_odp.02: |
| Parameter ac-01\_odp.03: a Microsoft-wide |
| Parameter ac-01\_odp.04: the Microsoft Information Risk Management Council (IRMC) organization |
| Parameter ac-01\_odp.05: at least annually |
| Parameter ac-01\_odp.06: significant changes |
| Parameter ac-01\_odp.07: at least annually |
| Parameter ac-01\_odp.08: significant changes |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☒ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AC-1 What is the solution and how is it implemented?** |
| **Part A1**  **Customer Responsibility**  The customer is responsible for developing, documenting, and disseminating access control policy and procedures that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.  **Azure**  Azure addresses the access control policy as part of the Microsoft security policies, of which there are two sets: the Microsoft Security Policy (MSP) that is applicable to all Microsoft personnel, and the Microsoft Security Program Policy (MSPP), which is applicable to all Microsoft personnel that have a responsibility for security. The Microsoft Information Risk Management Council (IRMC) is the governance body with review and approval responsibility for the MSP and MSPP. Within Azure, the MSPP specifically applies to all Microsoft personnel with security objectives such as designing, building, and operating Azure and across all information and processes used in the conduct of Microsoft business. All Azure personnel are accountable and responsible for complying with these guiding principles within their designated roles. The policy addresses the following:  \* Access control  \* Segregation of duties  Additionally, the policy addresses the purpose, scope, roles, responsibilities, compliance requirements, and required coordination among the various Microsoft organizations that provide some level of support to all services. The policies indicate Microsoft management’s commitment and are a component of the risk management strategy which provides Azure personnel with a current set of clear and concise information security requirements.  The MSP is available to all Microsoft personnel on the Microsoft Policy website on the Microsoft intranet, and the MSPP and Security Standards are available through the Liquid tool, also on the Microsoft intranet.  Service teams may supplement the Azure policies and procedures with offering-specific policies and procedures. Service-team-specific policies and procedures associated with access control are documented and stored within internal Azure SharePoint sites. Only personnel with authorized credentials, adequate levels of permission, legitimate need to know, and specific roles and responsibilities are given access to the service-team-specific policies or procedures. |
| **Part A2**  **Customer Responsibility**  The customer is responsible for procedures to facilitate the implementation of the access control policy and procedures and the associated access controls.  **Azure**  The Azure Access Control Standard Operating Procedure (SOP) implements the access control policy and associated controls and documents the following procedures:  \* Provisioning of Access  \* Modification and Review of Access Rights  \* Privilege Management  \* Inactive User Account Review  \* Separation of Duties  \* Remote Access Mechanisms  \* Session Control Parameters  Service teams may supplement the Azure policies and procedures with offering-specific policies and procedures. Service-team-specific policies and procedures associated with access control are documented and stored within internal Azure SharePoint sites. Only personnel with authorized credentials, adequate levels of permission, legitimate need to know, and specific roles and responsibilities are given access to the service-team-specific policies or procedures. |
| **Part B**  **Customer Responsibility**  The customer is responsible for designating an official to manage the development, documentation, and dissemination of the access control policy and procedures.  **Azure**  The Microsoft Information Risk Management Council (IRMC) organization is the governance body with approval responsibility for the Microsoft Security Policy (MSP) and Microsoft Security Program Policy (MSPP). The IRMC consists of representatives from security and risk management teams across Microsoft including Core Services Engineering and Operations (CSEO), Azure, and Global Security. The Customer Security and Trust: Security Engineering (CST-SE) organization manages the review and approval process and maintains the policies.  On an annual basis, the CST-SE conducts a line-by-line review of the MSP and MSPP. The Microsoft Security Policy (MSP) and Microsoft Security Program Policy (MSPP) Governance document describes each member’s role, types and frequency of review, escalation paths, approval process, and formal publishing procedures of the security policy. Throughout the year, if necessary, CST-SE may convene with the IRMC to conduct reviews after a significant review or change request. The approved policy update is published within the relevant tool on the Microsoft intranet. If service teams establish service-specific or team-specific policies, the respective service teams update the necessary policies at least annually. |
| **Part C1**  **Customer Responsibility**  The customer is responsible for reviewing and updating the current access control policy on a regular basis and following organization defined events.  **Azure**  The Azure team updates the Azure SOPs at least annually through a formal review process. If needed, the Azure team updates the SOP after a significant change affecting policy execution as well. If established, service-team-specific procedures are updated by their respective teams. The individual service teams review and update their respective SOPs at least annually and when required by a significant change. |
| **Part C2**  **Customer Responsibility**  The customer is responsible for reviewing and updating the current access control procedures on a regular basis and following organization defined events.  **Azure**  The Azure team updates the Azure SOPs at least annually through a formal review process. If needed, the Azure team updates the SOP after a significant change affecting policy execution as well. If established, service-team-specific procedures are updated by their respective teams. The individual service teams review and update their respective SOPs at least annually and when required by a significant change. |

## AC-2 Account Management

a. Define and document the types of accounts allowed and specifically prohibited for use within the system;

b. Assign account managers;

c. Require [prerequisites and criteria for group and role membership are defined;] for group and role membership;

d. Specify:

1. Authorized users of the system;

2. Group and role membership; and

3. Access authorizations (i.e., privileges) and [attributes (as required) for each account are defined;] for each account;

e. Require approvals by [personnel or roles required to approve requests to create accounts is/are defined;] for requests to create accounts;

f. Create, enable, modify, disable, and remove accounts in accordance with [policy, procedures, prerequisites, and criteria for account creation, enabling, modification, disabling, and removal are defined;];

g. Monitor the use of accounts;

h. Notify account managers and [personnel or roles to be notified is/are defined;] within:

1. [twenty-four (24) hours] when accounts are no longer required;

2. [eight (8) hours] when users are terminated or transferred; and

3. [eight (8) hours] when system usage or need-to-know changes for an individual;

i. Authorize access to the system based on:

1. A valid access authorization;

2. Intended system usage; and

3. [attributes needed to authorize system access (as required) are defined;];

j. Review accounts for compliance with account management requirements [monthly for privileged accessed, every six (6) months for non-privileged access];

k. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; and

l. Align account management processes with personnel termination and transfer processes.

|  |
| --- |
| **AC-2 Control Summary Information** |
| Responsible Roles: JIT, OneIdentity, Network Access Control, HR |
| Parameter ac-02\_odp.01: screening, training, and access conditions |
| Parameter ac-02\_odp.02: Role-Based Access Control (RBAC) attributes |
| Parameter ac-02\_odp.03: Staff account approvals conducted with account management tool |
| Parameter ac-02\_odp.04: Staff account management lifecycle enforced through account management tools |
| Parameter ac-02\_odp.05: Staff account changes enforced with account management tools |
| Parameter ac-02\_odp.06: Staff account changes enforced within 24 hours |
| Parameter ac-02\_odp.07: Staff account changes enforced within 8 hours |
| Parameter ac-02\_odp.08: Staff account changes enforced within 8 hours |
| Parameter ac-02\_odp.09: Staff account lifecycle managed through account management tools with Role-Based Access Control (RBAC) principles |
| Parameter ac-02\_odp.10: Staff accounts reviewed quarterly and elevated access is limited to specific dureation of time using JIT |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☒ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AC-2 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  The customer is responsible for defining and documenting all customer-controlled account types and accounts within the system. Customers configure Azure through either the Azure Management Portal or the Service Management API (SMAPI). These methods allow customers to create, modify, remove, and monitor storage accounts, hosted services, tenants, roles, and role instances within their subscription.  **Azure**  Azure accounts are only provided to Microsoft personnel supporting Azure services. Accounts with permissions to internal Azure assets and resources are not provisioned to customers.  Azure uses Active Directory (AD) to manage access to implement Role-Based Access Control (RBAC) using AD groups. Microsoft personnel are assigned unique corporate network (CorpNet) AD accounts as part of a standard onboarding to Microsoft. These CorpNet accounts, known as a user's alias, do not have access to any Azure domains by default.  For personnel supporting Azure services, a user account within each Azure domain ties to the user's CorpNet account using his or her unique CorpNet alias. This alias is consistent across all a user's accounts in all Microsoft domains, including Azure. CorpNet and Azure access are provisioned and managed using separate account management tools. Azure utilizes OneIdentity for both identifier and security group management.  Azure utilizes the Global Management Environment (GME) and Azure Management Environment (AME) domains for access to Azure. Each domain is specific to the environment. As an example, John Doe's alias is jdoe, with accounts jdoe@redmond.com for access to CorpNet and jdoe@ame.gbl for access to Azure Commercial. Below are the different account types that Azure utilizes.  **Standard Access**  All personnel with standard access to Azure are granted system metadata read access used for regular troubleshooting, release management, and other maintenance and monitoring activities. Standard access provides permissions to key Azure tools, services, SharePoint sites, documentation, and a variety of dashboards.  For instance, a user with standard access may have the need to review service-specific logs within Azure to identify and diagnose issues. These accounts are considered unprivileged due to the lack of write access. Any additional permissions above standard access requires elevation of access via the Azure Just in Time (JIT) tool, described below.  **Elevated Access**  All personnel must use JIT when interactive elevated access is required in the Azure production environment. Except in the case of an approved exception as described below, there is no standing or persistent elevated access to the Azure production environment. The primary exception is Break-Glass elevated access, described below.  In scenarios where JIT does not yet support management of elevated access, standing access may exist; these gaps in JIT support are identified and tracked as an exception, which requires approval. Software deployment via automated means (i.e., not using an interactive login) does not require interactive login to a resource that is accessed via JIT. In this case, a service team member submits a job (e.g., Pull Request in Azure DevOps), and another team member reviews, approves, and then the safe deployment system deploys.  **Elevated Access – Break-Glass Access**  Azure maintains Break-Glass accounts with elevated access for use in the scenario that the JIT service is not available. These accounts have persistent elevated access to perform maintenance activities if JIT is unable to provide temporary elevated access. These accounts are carefully managed, only to be used in emergencies, and have notifications associated with their use. Whenever such an account is utilized, a Severity 2 incident ticket is generated that requires the service that owns the resource to investigate and determine whether the access is valid.  **Network Device Accounts**  Access to network devices is managed through the Authentication, Authorization, and Accounting (AAA) system, which is configured to allow a specific role-based level of access to Azure Networking network devices via specific AD security groups managed by Azure Networking. There are no user accounts or groups configured in the AAA system, as account and security group access is managed and inherited from the Active Directory infrastructure, with AAA acting as its own directory for the leveraged accounts. The AAA system provides automated mechanisms to support accounts in use for network device access, including integration with network devices for administration access control, and allows for centralized control and auditing of administrative actions in the environment. For privileged access, a JIT request is required which grants Read Write (RW) access.  **Service Accounts**  Non-user, non-interactive service accounts are used to run relevant services. Service accounts are not used for interactive logins. For example, software deployment via automated means does not require interactive login to a resource that would normally be accessed via JIT. In this example, a service team member submits a job, such as a Pull Request in Azure DevOps, and another team member reviews and approves, at which point the Azure Safe Deployment Practices (SDP) automatically deploys.  **Group, Anonymous, and Temporary Accounts**  Group or shared accounts are not utilized within Azure unless necessary, where a local account cannot be deleted or disabled or is necessary for Break-Glass access. For accounts tracked as approved exceptions, the credentials are stored in an approved secret management store, which tracks and monitors access to the credentials and ensures group or shared account usage is uniquely attributable to the user accessing it. This is accomplished by associating the secret store logs with the group or shared account usage. When a user accesses the credentials in the secret management store, that user is uniquely identified, ensuring non-repudiation and attributing user activity to the shared account. |
| **Part B**  **Customer Responsibility**  The customer is responsible for assigning managers to the accounts identified in AC-02 Part a.  **Azure**  All account approvals for Azure go through OneIdentity. All security groups have a primary and secondary owner identified. When a user submits a request, these approvers receive a notification to approve or deny. |
| **Part C**  **Customer Responsibility**  The customer is responsible for establishing role and group membership criteria for customer-controlled account types.  **Azure**  When an Azure user requests access to any security group, the request is approved by the owner of the group based on the criteria defined for membership. Azure has certain environment-wide conditions, such as screening and training completion, that are met before receiving any Azure account. Additional conditions and criteria are established by the service team. All conditions are enforced by OneIdentity. |
| **Part D**  **Customer Responsibility**  The customer is responsible for establishing role and group membership criteria for customer-controlled account types.  **Azure**  The Azure service team's management identifies service team personnel who should be given authorization to access the system and specifies the type of privilege each service team personnel should have based on their role. Azure utilizes Role-Based Access Control (RBAC) to identify and control the access privileges of each service team user in accordance with OneIdentity restrictions. Access privileges vary depending on the role a specified service team member assumes within the service team. Access privileges are defined by the service teams in OneIdentity and enforced by Active Directory. |
| **Part E**  **Customer Responsibility**  The customer is responsible for requiring personnel to approve the creation of new accounts for the system.  **Azure**  All account approvals in Azure, including establishing user accounts, security groups, and service accounts, go through OneIdentity. No access is possible without an approved account. When a user submits a request, the approver identified in AC-02 Part c receives an email notification. Approvers may also go directly to the tool to view a request. The approver follows these steps to approve or deny the request ticket and determine the level of user access:  \* The approver determines whether the business justification is sufficient.  \* The approver determines whether the level of user access requested is appropriate.  The approver adheres to the principles of least privilege and separation of duties when approving and assigning user access rights and can reject or modify the requested permissions if they are not appropriate. In the case of access requests to multiple services, this may translate into different levels of permissions against the different services to which the user needs access. |
| **Part F**  **Customer Responsibility**  The customer is responsible for establishing an account management process for all customer-controlled account types. Azure can sync user entities and groups allowing them to be used to permission users to resources in Azure.  **Azure**  Azure personnel are assigned unique corporate network (CorpNet) Active Directory (AD) accounts by Core Services Engineering and Operations (CSEO) as part of a standard onboarding to Microsoft. All Azure access requests and approvals leverage these CorpNet identifiers and are managed through OneIdentity, which is an account provisioning tool that tracks the process for account request, approval, creation, modification, and deletion. New user accounts refer to accounts of existing Microsoft users using their unique CorpNet identifiers, known as aliases, who require access to Azure resources.  Standard Access permits authorized users persistent access to a service’s documentation, work items, source code, telemetry, reports, and KPIs, and to submit and/or process deployment jobs using dual-key. Service team approvers create, enable, modify, disable, and remove group memberships that grant this access using OneIdentity. Elevated access to the Azure production environment is primarily either dual-key (one user submits, another reviews and approves or rejects) for automation or uses Just In Time (JIT) approvals for interactive user access. JIT provides personnel elevated access for a defined period to resolve LiveSite or deployment incidents. Azure has automated the JIT access request process through the JIT portal by defining policies for access provisioning and revocation. Service teams must define a JIT policy indicating which users may request JIT elevation, the duration of that elevation, and the scope of elevation. The default duration is eight (8) hours, with a maximum of twenty four (24) hours. JIT policy changes are dual-key. The user initiates the access request by logging into the JIT portal and submitting the JIT access request. The access request submitted through the JIT portal is first adjudicated by system policies, then further evaluated against policies defined by the service that owns the resource – which could immediately deny the request, approve the request if conditions are met, or route the request to appropriate team members based on workflow configured in the service team policy, which is also dual-key.  Barring any approved exceptions – including those approved due to lack of JIT support, the only persistent elevated access permitted to the Azure production environment is JIT Break-Glass access, which alerts the resource owner when invoked.  Azure account authorizers review accounts quarterly. Additionally, when a user is promoted or transferred to another group, the account authorizers review and modify or revoke as necessary user role and access rights according to the access policies. Furthermore, OneIdentity automatically terminates access depending on the rules configured for the project and the new manager’s approval if not manually approved after transfer. The user is required to resubmit a request for access when that individual’s access is close to expiring.  For additional protection, Azure Security Monitoring (ASM) and SCUBA monitor service team operating systems for unexpected account creations. This includes monitoring for if an administrator or privileged role is added to an Azure subscription at the operating system layer, intended to prevent persistent access from bypassing the JIT process.  When a user leaves the company, their manager or their manager’s work-on-behalf will submit the user’s resignation in the Employee Central system. Subsequently, an automatic notification is sent to the HR Administrator and the user. The user’s resignation includes the user’s last working day. If the last working day needs to be changed, the user’s manager or HR administrator will take the action to change the date in the HR database. On the employee's last working day, information automatically flows to the HR database to ensure accounts tied to their CorpNet credentials are disabled. On the user’s last day, referred to as the termination date, access is shut off automatically since the Employee Central (EC) system is tied to the SAP systems; the user’s status switches to inactive and they are removed from payroll and benefits. If the user is leaving for a competitor, their access to the environment and buildings is terminated within forty-eight (48) hours of their notification to terminate.  OneIdentity disables any user accounts daily if no HR record exists within the EC system, such as after termination, or if the accounts have been inactive over one hundred and eight (180) days. Accounts that have been disabled for fifteen (15) days after one hundred and eight (180) days of inactivity are deleted. Accounts can be disabled upon request in OneIdentityand MyAccess.  If a user’s account doesn’t exist in the HR system, due to employment termination, for example, or if the account has been inactive over one hundred and eight (180) days OneIdentity will delete the AD object associated with the user’s alias, thereby, disabling any permissions previously assigned. Accounts that have been disabled for fifteen (15) days after one hundred and eight (180) days of inactivity are deleted. Accounts can be manually disabled upon request in OneIdentity and MyAccess. |
| **Part G**  **Customer Responsibility**  The customer is responsible for monitoring the use of all customer-controlled accounts.  **Azure**  Azure monitors the use of information system accounts using the audit logging and monitoring pipeline. This includes the appropriate configuration of local log settings, the central collection of log data, and the detection and alerting of suspicious activity. |
| **Part H1**  **Customer Responsibility**  The customer is responsible for notifying customer account managers defined in AC-02 Part b of all customer-controlled accounts when users are terminated or transferred, accounts are no longer required, or system usage or need-to-know changes.  All customers in the Azure environment that use identity federation are responsible for having a process in place for account management of their users including creating new user accounts for new employees, reviewing accounts periodically, modifying access in accordance with changes to employee job responsibilities, and disabling the accounts of terminated employees. The processes should be automatically audited, and notifications should be sent to appropriate individuals as required. Changes made to users’ permissions in the customer AD are reflected in the claim presented via ADFS the next time a user is authenticated.  **Azure**  When a user leaves the company, their manager or their manager’s work-on-behalf will submit the user’s resignation in the Employee Central system. Subsequently, an automatic notification is sent to the HR administrator. The Employee Central system also automatically notifies Core Services Engineering and Operations (CSEO) and the Global Security Group of the user’s last working day. The user’s resignation includes the user’s last working day. If the last working day needs to be changed, the user’s manager or HR administrator will take the action to change the date in the HR database. The last working day information automatically flows to the HR database to ensure accounts tied to their CorpNet credentials are disabled on the user’s last working day. For urgent terminations, the HR administrator will also notify Core Services Engineering and Operations (CSEO) outside of the Employee Central notification window to initiate immediate action to disable access. As a result, Azure user accounts are disabled upon the user’s last working day or during the time when access is requested to be disabled.  When a user is promoted or transferred to another group, the user role and access rights are reviewed and revoked according to the access policy. The user profile is changed after proper approvals and authorization from the respective group owners.  Accounts of terminated users and transferred users are deactivated after confirmation from the appropriate manager. User accounts are evaluated daily to determine if they are actively employed by Microsoft. The OneIdentity Life Cycle Management job is run daily to disable any user accounts within Azure domains if there is no HR record or if they have been inactive over one hundred and eighty (180) days. Azure receives a daily HR feed of personnel, which it compares to the list of Azure domain users. Any user accounts that do not have a matching HR record have had a position change in the HR record or have been flagged as inactive are then disabled by the tools. |
| **Part H2**  **Customer Responsibility**  The customer is responsible for notifying customer account managers defined in AC-02 Part b of all customer-controlled accounts when users are terminated or transferred, accounts are no longer required, or system usage or need-to-know changes.  All customers in the Azure environment that use identity federation are responsible for having a process in place for account management of their users including creating new user accounts for new employees, reviewing accounts periodically, modifying access in accordance with changes to employee job responsibilities, and disabling the accounts of terminated employees. The processes should be automatically audited, and notifications should be sent to appropriate individuals as required. Changes made to users’ permissions in the customer AD are reflected in the claim presented via ADFS the next time a user is authenticated.  **Azure**  When a user leaves the company, their manager or their manager’s work-on-behalf will submit the user’s resignation in the Employee Central system. Subsequently, an automatic notification is sent to the HR administrator. The Employee Central system also automatically notifies Core Services Engineering and Operations (CSEO) and the Global Security Group of the user’s last working day. The user’s resignation includes the user’s last working day. If the last working day needs to be changed, the user’s manager or HR administrator will take the action to change the date in the HR database. The last working day information automatically flows to the HR database to ensure accounts tied to their CorpNet credentials are disabled on the user’s last working day. For urgent terminations, the HR administrator will also notify Core Services Engineering and Operations (CSEO) outside of the Employee Central notification window to initiate immediate action to disable access. As a result, Azure user accounts are disabled upon the user’s last working day or during the time when access is requested to be disabled.  When a user is promoted or transferred to another group, the user role and access rights are reviewed and revoked according to the access policy. The user profile is changed after proper approvals and authorization from the respective group owners.  Accounts of terminated users and transferred users are deactivated after confirmation from the appropriate manager. User accounts are evaluated to determine if they are actively employed by Microsoft daily. The OneIdentity Life Cycle Management job is run to disable any user accounts within Azure domains daily if there is no HR record or have been inactive over one hundred and eighty (180) days. Azure receives a daily HR feed of personnel, which it compares to the list of Azure domain users. Any user accounts that do not have a matching HR record have had a position change in the HR record or have been flagged as inactive are then disabled by the tools. |
| **Part H3**  **Customer Responsibility**  The customer is responsible for notifying customer account managers defined in AC-02 Part b of all customer-controlled accounts when users are terminated or transferred, accounts are no longer required, or system usage or need-to-know changes.  All customers in the Azure environment that use identity federation are responsible for having a process in place for account management of their users including creating new user accounts for new employees, reviewing accounts periodically, modifying access in accordance with changes to employee job responsibilities, and disabling the accounts of terminated employees. The processes should be automatically audited, and notifications should be sent to appropriate individuals as required. Changes made to users’ permissions in the customer AD are reflected in the claim presented via ADFS the next time a user is authenticated.  **Azure**  When a user leaves the company, their manager or their manager’s work-on-behalf will submit the user’s resignation in the Employee Central system. Subsequently, an automatic notification is sent to the HR administrator. The Employee Central system also automatically notifies Core Services Engineering and Operations (CSEO) and the Global Security Group of the user’s last working day. The user’s resignation includes the user’s last working day. If the last working day needs to be changed, the user’s manager or HR administrator will take the action to change the date in the HR database. The last working day information automatically flows to the HR database to ensure accounts tied to their CorpNet credentials are disabled on the user’s last working day. For urgent terminations, the HR administrator will also notify Core Services Engineering and Operations (CSEO) outside of the Employee Central notification window to initiate immediate action to disable access. As a result, Azure user accounts are disabled upon the user’s last working day or during the time when access is requested to be disabled.  When a user is promoted or transferred to another group, the user role and access rights are reviewed and revoked according to the access policy. The user profile is changed after proper approvals and authorization from the respective group owners.  Accounts of terminated users and transferred users are deactivated after confirmation from the appropriate manager. User accounts are evaluated to determine if they are actively employed by Microsoft daily. The OneIdentity Life Cycle Management job is run to disable any user accounts within Azure domains daily if there is no HR record or have been inactive over one hundred and eighty (180) days. Azure receives a daily HR feed of personnel, which it compares to the list of Azure domain users. Any user accounts that do not have a matching HR record have had a position change in the HR record or have been flagged as inactive are then disabled by the tools. |
| **Part I1**  **Customer Responsibility**  The customer is responsible for authorizing access to the customer system.  **Azure**  OneIdentity enables role-based access to Azure’s production network and supporting infrastructure in a secure manner that complies with least privilege policies and guidelines set by Microsoft. Access requests and modifications to Azure security groups and thus privileges in the Azure environment are approved based upon meeting criteria that determine the appropriateness of the requested role and is completed by an account approver based on rules defined in OneIdentity.  Information system usage or need-to-know/need-to-share changes are managed by the owner of the service. The service owner and account approvers can request changes to the access of accounts on their service for AD accounts through OneIdentity. |
| **Part I2**  **Customer Responsibility**  The customer is responsible for authorizing access to the customer system.  **Azure**  OneIdentity enables role-based access to Azure’s production network and supporting infrastructure in a secure manner that complies with least privilege policies and guidelines set by Microsoft. Access requests and modifications to Azure security groups and thus privileges in the Azure environment are approved based upon meeting criteria that determine the appropriateness of the requested role and is completed by an account approver based on rules defined in OneIdentity.  Information system usage or need-to-know/need-to-share changes are managed by the owner of the service. The service owner and account approvers can request changes to the access of accounts on their service for AD accounts through OneIdentity. |
| **Part I3**  **Customer Responsibility**  The customer is responsible for authorizing access to the customer system.  **Azure**  OneIdentity enables role-based access to Azure’s production network and supporting infrastructure in a secure manner that complies with least privilege policies and guidelines set by Microsoft. Access requests and modifications to Azure security groups and thus privileges in the Azure environment are approved based upon meeting criteria that determine the appropriateness of the requested role and is completed by an account approver based on rules defined in OneIdentity.  Information system usage or need-to-know/need-to-share changes are managed by the owner of the service. The service owner and account approvers can request changes to the access of accounts on their service for AD accounts through OneIdentity. |
| **Part J**  **Customer Responsibility**  The customer is responsible for reviewing customer-controlled accounts at the required frequency to determine if accounts are compliant with all organization requirements.  **Azure**  Access is based on specific roles and duties to support the operational environments. The foundation is granting elevated access for a limited duration through JIT not to exceed twenty-four (24) hours; and a formal program that monitors account activities enabled by auditing account management actions. This provides ongoing review of accounts and alerts of changes. The objective is a continuous rather than static review of access authorizations and activities.  There is no standing privileged access to the Azure production environment. Azure utilizes Just in Time (JIT) access and Break-Glass accounts for the implementation of this control. Individuals request elevated access for a specific, limited purpose. Upon approval, JIT grants temporary audited access on the Azure asset (e.g., assign RBAC role, assign claim, generate account and assign to the local administrator group on a virtual machine, etc.). The access is automatically revoked after a set limited time and all access grants are securely audited using the JIT system and/or destination resource logging mechanisms. JIT terminates access based on the rules configured in the adjudicating policy, as defined by the resource owner. Once a JIT grant has expired, the access will be revoked and the user must submit a new request for access if access is still required. Because no JIT access is provided exceeding twenty-four (24) hours, and all JIT requests are reviewed prior to approval either manually or via automated rules set by the owning service team, the intent of this requirement is met.  Break-Glass accounts, which have persistent elevated access to the production environment, are only utilized in Break-Glass situations when JIT is inaccessible. The use of these accounts generates a Severity 2 ticket, which requires review immediately, meeting the intent of the requirement.  Microsoft also executes a Quarterly Access Review (QAR) of all accounts each quarter. A full inventory of accounts is analyzed with the managers of each account identified. Managers are required to revalidate access for an account to remain active. If a manager indicates an account is no longer necessary, or a manager does not respond, the account is deactivated. |
| **Part K**  **Customer Responsibility**  The customer is responsible for the management of customer-controlled shared/group account credentials when a user is removed from the shared/group account.  **Azure**  Group or shared accounts are not utilized within Azure unless necessary, such as where the local account or accounts cannot be deleted or disabled, or where necessary for Break-Glass access. For accounts tracked as approved exceptions, the credentials are stored in an approved secret management store, which tracks and monitors access to secrets and ensures group or shared account usage is uniquely attributable to the user accessing it by associated the secret store logs with the group or shared account usage. When a user accesses the credentials in the secret management store, that user is identified uniquely, ensuring non-repudiation and attributing user activity to the shared account. |
| **Part L**  **Customer Responsibility**  The customer is responsible for aligning account management processes with personnel termination and transfer processes for customer-deployed resources.  **Azure**  Azure aligns account management processes with personnel termination and transfer processes. When a user leaves the company, their manager or their manager’s work-on-behalf will submit the user’s resignation in the Employee Central system. Subsequently, an automatic notification is sent to the HR Administrator and the user. The user’s resignation includes the user’s last working day. If the last working day needs to be changed, the user’s manager or HR administrator will take the action to change the date in the HR database. The last working day information automatically flows to the HR database to ensure accounts tied to their CorpNet credentials are disabled on the user’s last working day. On the user’s last day, referred to as the termination date, access is shut off automatically since the Employee Central (EC) system is tied to the SAP systems; the user’s status switches to inactive and they are removed from payroll and benefits. If the user is leaving for a competitor, their access to the environment and buildings is terminated within forty-eight (48) hours of their notification to terminate. When a user is promoted or transferred to another group, the user role and access rights are reviewed and revoked according to the access policy. The user profile is changed after proper approvals and authorization from the respective group owners.  Accounts of terminated users are deactivated automatically upon OneIdentity’s sync with SAP HR system. Transferred users are deactivated after confirmation from the appropriate manager. User accounts are evaluated to determine if they are actively employed by Microsoft daily. The OneIdentity Life Cycle Management job is run to disable any user accounts within Azure domains daily if there is no HR record or have been inactive over one hundred and eighty (180) days. Azure receives a daily HR feed of personnel, which it compares to the list of Azure domain users. Any user accounts that do not have a matching HR record have had a position change in the HR record or have been flagged as inactive are then disabled by the tools. |

### AC-2(1) - Automated System Account Management

Support the management of system accounts using [automated mechanisms used to support the management of system accounts are defined; ].

|  |
| --- |
| **AC-2(1) Control Summary Information** |
| Responsible Roles: JIT, OneIdentity |
| Parameter ac-02.01\_odp: MyAccess, OneIdentity, JIT |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AC-2(1) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for supporting the management of system accounts using organization-defined automated mechanisms.  **Azure**  Microsoft provisions and manages Azure access using a number of automated mechanisms; specifically, MyAccess for CorpNet access and OneIdentity and JIT for access to the Azure cloud. Access to Microsoft's corporate network CorpNet and access to the Azure cloud are provisioned and managed using separate account management tools. Microsoft's CorpNet account management, using the MyAccess tool, cannot provide access to Azure – it can only provide access to Active Directory (AD) security groups that the Azure account management tool, OneIdentity, leverages.  All Azure access requests and approvals are managed through JIT using OneIdentity accounts. OneIdentity is a provisioning tool for accounts used to access Azure cloud. It tracks account requests, approvals, creations, modifications, and deletions.  Azure uses Just in Time (JIT) access for privileged access to Azure. Microsoft personnel request access for a specific, limited purpose. Upon approval, JIT grants temporary, audited membership to the local administrator group or elevated role (e.g. Subscription Owner, Contributor, etc.). The membership is automatically revoked after a limited duration defined by the JIT policy, and all access grants are securely audited. |

### AC-2(2) - Automated Temporary and Emergency Account Management

Automatically [Selection: remove;disable] temporary and emergency accounts after [no more than 24 hours from last use].

|  |
| --- |
| **AC-2(2) Control Summary Information** |
| Responsible Roles: JIT, OneIdentity |
| Parameter ac-02.02\_odp.01: Not applicable |
| Parameter ac-02.02\_odp.02: Not applicable |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☒ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☒ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AC-2(2) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for configuring the system to automatically remove or disable emergency and temporary accounts. User entities are responsible for having a process in place for account management of their users by creating new user accounts for new employees, modifying access in accordance with changes to employee job responsibilities, and disabling the accounts of terminated employees. The processes should be automatically audited, and notifications should be sent to appropriate individuals as required. Customer authentication requests are processed by the customer authentication environment; when an employee is terminated in the customer environment they are no longer able to authenticate to Azure.  **Azure**  The Microsoft Security Program Policy (MSPP) prohibits the use of temporary and emergency accounts. All local guest accounts are disabled on the system or platform wherever they are located. All account requests follow the standard account management process, including domain account request and approval and OneIdentity-based group management.  For servers that are not domain-joined, the JIT process for granting access to a server includes creating and enabling a local account for the duration of access. Because this access is tied to a specific user’s domain account and requires that the user first authenticate using multifactor authentication, Azure does not consider this local account to be a temporary account for purposes of this control. |

### AC-2(3) - Disable Accounts

Disable accounts within [24 hours for user accounts] when the accounts:

(a) Have expired;

(b) Are no longer associated with a user or individual;

(c) Are in violation of organizational policy; or

(d) Have been inactive for [thirty-five (35) days (See additional requirements and guidance.)].

Requirement: The service provider defines the time period for non-user accounts (e.g., accounts associated with devices). The time periods are approved and accepted by the JAB/AO. Where user management is a function of the service, reports of activity of consumer users shall be made available.

(d) Requirement: The service provider defines the time period of inactivity for device identifiers.

Guidance: For DoD clouds, see DoD cloud website for specific DoD requirements that go above and beyond FedRAMP https://public.cyber.mil/dccs/.

|  |
| --- |
| **AC-2(3) Control Summary Information** |
| Responsible Roles: OneIdentity |
| Parameter ac-02.03\_odp.01: 90 days for AME; 84 days for GME |
| Parameter ac-02.03\_odp.02: 90 days for AME; 84 days for GME |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AC-2(3) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for configuring the system to automatically disable user accounts that have expired, are no longer associated with a user or individual, are in violation of organizational policy, or are inactive.  **Customer Identity Federation**  User entities are responsible for having a process in place for account management of their users by creating new user accounts for new employees, modifying access in accordance with changes in employee job responsibilities, and disabling the accounts of terminated employees. The processes should be automatically audited, and notifications should be sent to appropriate individuals as required. Since user entities are authenticated by authentication systems and federated via ADFS when the users are terminated from the federal authentication provider they also lose access to Azure. User entities are responsible for automatically disabling Azure accounts when the accounts are inactive or no longer used.  **Azure**  User accounts are automatically evaluated to determine if they are actively being used by Microsoft users. OneIdentity receives a daily HR feed of personnel, which it compares to the list of users. Any user accounts that do not have a matching HR record or have been flagged as inactive are then disabled by this process.  The OneIdentity process is used to disable any user accounts within AME and GME on a daily basis if there are no associated HR records, or the user accounts have been inactive over 90 for AME, 84 for GME days. All accounts are automatically disabled after the required number of days.  Inactive service accounts are never disabled. In an Active Directory environment, all service account IDs are completely unique. It is not possible to reuse or spoof a service account ID. There is no risk mitigated by retiring or disabling service account IDs. |

### AC-2(4) - Automated Audit Actions

Automatically audit account creation, modification, enabling, disabling, and removal actions.

|  |
| --- |
| **AC-2(4) Control Summary Information** |
| Responsible Roles: OneIdentity, Network Access Control, Logging and Monitoring |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AC-2(4) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for automatically auditing account creation, modification, enabling, disabling, and removal actions.  **Azure**  OneIdentity, which is used to manage all Azure domain accounts, automatically logs account creation, modification, and disablement actions which are ingested into Geneva Monitoring.  **Servers**  Azure performs auditing of elevated user accounts at the asset layer through Geneva Monitoring. The servers provide a record of account creation, modification, disabling, and termination of accounts, which notifies the Security Response Team for any suspicious activities.  **Network Devices**  Network device access is audited via logs from the Authentication, Authorization, and Accounting (AAA) system. The AAA logs AAA Administration, which includes account creation, modification, and disablement. |

### AC-2(5) - Inactivity Logout

Require that users log out when [inactivity is anticipated to exceed Fifteen (15) minutes].

Guidance: Should use a shorter timeframe than AC-12.

|  |
| --- |
| **AC-2(5) Control Summary Information** |
| Responsible Roles: Corporate IT |
| Parameter ac-02.05\_odp: at the end of the user’s standard work period, in advance of any expected unattended inactivity exceeding fifteen (15) minutes, when the task for which the user logged on is complete, or when JIT access expires |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AC-2(5) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for defining and enforcing an inactivity log out policy.  **Azure**  Azure requires that all personnel log out at the end of their work period, in advance of any expected unattended inactivity exceeding fifteen (15) minutes, or when they have completed the task that was the purpose of the login, including at the end of their workday. Additionally, when a user has elevated to administrative access using the JIT process, that user’s connections are automatically terminated upon expiration of the elevation. |

### AC-2(7) - Privileged User Accounts

(a) Establish and administer privileged user accounts in accordance with [Selection: a role-based access scheme;an attribute-based access scheme] ;

(b) Monitor privileged role or attribute assignments;

(c) Monitor changes to roles or attributes; and

(d) Revoke access when privileged role or attribute assignments are no longer appropriate.

|  |
| --- |
| **AC-2(7) Control Summary Information** |
| Responsible Roles: JIT, OneIdentity, Network Access Control |
| Parameter ac-02.07\_odp: actions to disable or revoke the elevated user account or remove it from relevant security groups immediately |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AC-2(7) What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  The customer is responsible for administering elevated user accounts using a role-based access scheme (for customer-controlled accounts). Federated user entities are responsible for enforcing RBAC within their own Active Directory infrastructure and monitoring those role assignments to meet internal requirements.  **Azure**  Administrative access within Azure uses the JIT process, which grants temporary administrative access through AD security groups, subscription roles, and temporary accounts created with RBAC permissions applied, and Break-Glass accounts, which utilize AD security groups for administrative access but create Severity 2 alerts when used. Using these methods, Azure personnel establish elevated access in accordance with a role-based access scheme, which organizes information system privileges into roles that are assigned to AD security groups of which users become a member.  For the persistent accounts that are exceptions to the JIT and Break-Glass implementations, any group membership action that provides elevated persistent access to Azure is provisioned only after explicit approval by asset owners based on the role of the requestor. This access restriction is strictly enforced via security groups, where security group owners determine approval to be added to a security group based on business justification and role of a user. |
| **Part B**  **Customer Responsibility**  The customer is responsible for monitoring elevated roles of customer-controlled accounts.  **Azure**  Access requests to all AD security groups are tracked and managed by OneIdentity, MyAccess, and CoreIdentity. These tools track the process of security group access request, approval, creation, modification, and deletion for Azure identities.  All Azure production accounts are tracked and monitored using the automated account management tools including OneIdentity, MyAccess, and CoreIdentity and JIT, audit event collection and reporting, and administrative access audit reviews. Accounts are granted access to production system based on roles defined to limit the access to the services and privileges needed for the administrator to complete their job.  Azure tracks and monitors elevated role assignments through the access approval as needed for JIT, upon execution for Break-Glass accounts, and when requested as an exception to JIT and Break-Glass for persistent access. Azure also executes a quarterly review for all accounts, disabling those identified as unnecessary. |
| **Part C**  **Customer Responsibility**  The customer is responsible for monitoring elevated roles of customer-controlled accounts.  **Azure**  Access requests to all AD security groups are tracked and managed by OneIdentity, MyAccess, and CoreIdentity. These tools track the process of security group access request, approval, creation, modification, and deletion for Azure identities.  All Azure production accounts are tracked and monitored using the automated account management tools including OneIdentity, MyAccess, and CoreIdentity and JIT, audit event collection and reporting, and administrative access audit reviews. Accounts are granted access to production system based on roles defined to limit the access to the services and privileges needed for the administrator to complete their job.  Azure tracks and monitors elevated role assignments through the access approval as needed for JIT, upon execution for Break-Glass accounts, and when requested as an exception to JIT and Break-Glass for persistent access. Azure also executes a quarterly review for all accounts, disabling those identified as unnecessary. |
| **Part D**  **Customer Responsibility**  The customer is responsible for acting on customer-controlled accounts when elevated role assignments are no longer appropriate.  **Azure**  Elevated role assignments are no longer appropriate when Azure personnel either no longer need the administrative access to accomplish their task, their allotted JIT time expires, or the personnel are transferred or terminated. In those cases, Azure follows the account management processes to terminate the account or revoke access. |

### AC-2(9) - Restrictions on Use of Shared and Group Accounts

Only permit the use of shared and group accounts that meet [organization-defined need with justification statement that explains why such accounts are necessary].

Requirement: Required if shared/group accounts are deployed.

|  |
| --- |
| **AC-2(9) Control Summary Information** |
| Responsible Roles: OneIdentity, Network Access Control, Secret Management Stores |
| Parameter ac-02.09\_odp: these requirements: established for a clearly-defined administrative purpose that cannot be fulfilled using individual accounts and credentials stored in an approved secret management store which uniquely identifies usage of the shared account credentials and uniquely attributes user activity to the account |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☒ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AC-2(9) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for restricting the use of customer-controlled shared/group accounts.  **Azure**  Group or shared accounts are not utilized within Azure unless necessary, such as where the local account or accounts cannot be deleted or disabled, or where necessary for Break-Glass access. For accounts tracked as approved exceptions, the credentials for these accounts are stored in an approved secret management store, which tracks and monitors access to secrets and ensures group or shared account usage is uniquely attributable to the user accessing it by associated the secret store logs with the group or shared account usage. When a user accesses the credentials in the secret management store, that user is identified uniquely, ensuring non-repudiation and attributing user activity to the shared account. |

### AC-2(11) - Usage Conditions

Enforce [circumstances and/or usage conditions to be enforced for system accounts are defined;] for [system accounts subject to enforcement of circumstances and/or usage conditions are defined;].

|  |
| --- |
| **AC-2(11) Control Summary Information** |
| Responsible Roles: Azure Compliance |
| Parameter ac-02.11\_odp.01: Not applicable |
| Parameter ac-02.11\_odp.02: Not applicable |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☒ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☒ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AC-2(11) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for applying usage conditions or restrictions for any customer-controlled accounts.  **Azure**  Azure operates twenty-four (24) hours a day, seven (7) days a week, and as such, does not apply usage conditions or restrictions for any Azure accounts. |

### AC-2(12) - Account Monitoring for Atypical Usage

(a) Monitor system accounts for [atypical usage for which to monitor system accounts is defined;] ; and

(b) Report atypical usage of system accounts to [at a minimum, the ISSO and/or similar role within the organization].

(a) Requirement: Required for privileged accounts.

(b) Requirement: Required for privileged accounts.

|  |
| --- |
| **AC-2(12) Control Summary Information** |
| Responsible Roles: Incident Response |
| Parameter ac-02.12\_odp.01: indications of compromise detailed in the Azure Incident Management Standard Operating Procedure (SOP) |
| Parameter ac-02.12\_odp.02: personnel, teams, and roles identified in IR-06 |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AC-2(12) What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  The customer is responsible for monitoring customer-controlled accounts for atypical usage.  **Azure**  Azure monitors for atypical use by monitoring for the indications of compromise identified in the Azure Incident Management Standard Operating Procedure (SOP). |
| **Part B**  **Customer Responsibility**  The customer is responsible for reporting atypical behavior of customer-controlled accounts.  **Azure**  Azure follows normal incident reporting procedures if atypical use is detected, including reporting to the Security Response Team and ISSO/ISSM as necessary. |

### AC-2(13) - Disable Accounts for High-risk Individuals

Disable accounts of individuals within [one (1) hour] of discovery of [significant risks leading to disabling accounts are defined;].

|  |
| --- |
| **AC-2(13) Control Summary Information** |
| Responsible Roles: JIT, OneIdentity, Network Access Control |
| Parameter ac-02.13\_odp.01: one (1) hour |
| Parameter ac-02.13\_odp.02: indications of compromise detailed in the Azure Incident Management Standard Operating Procedure (SOP) |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AC-2(13) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for disabling customer-controlled accounts of users posing a significant risk within the appropriate timeframe.  **Azure**  Active monitoring tools include the Geneva Monitoring Agent (MA), System Center Operations Manager (SCOM), and Kusto. Audit records for each Azure service are captured by the MA and retained in Azure Storage. The MA aggregates monitoring information for review. SCOM provides file integrity validation and protection, as well as the recovery of core system files if any unauthorized changes are detected. Kusto consolidates all available logs.  These tools are configured to provide near-real-time alerts to service team or Security Response Team personnel in situations that require immediate action. Microsoft documents the indications of compromise or potential compromise in the Azure Incident Management Standard Operating Procedure (SOP). Azure follows normal incident reporting procedures if atypical usage is detected. Per the new hire orientation process, users that are discovered to pose a significant risk to Microsoft are terminated and their access is revoked from Microsoft networks, including Azure. For involuntary terminations, an urgent request for access termination is submitted via email from HR and access is disabled within four (4) hours. |

## AC-3 Access Enforcement

Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

|  |
| --- |
| **AC-3 Control Summary Information** |
| Responsible Roles: JIT, OneIdentity, Microsoft Entra ID (formerly AAD) |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AC-3 What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for enforcing approved authorizations for logical access to customer-deployed resources.  The customer is responsible for enforcing approved authorizations for logical access to the system, in compliance with their organizational policies, using their Active Directory (AD) infrastructure. Users authenticate to customer-owned ADFS servers which utilize the customer AD infrastructure to identify, authenticate, and apply permissions to that user’s session. The customer ADFS server then communicates that identification and authentication and associated permissions to Microsoft Entra ID (formerly AAD) via a SAML 2.0 ticket. Once permissions are communicated to Microsoft Entra ID (formerly AAD), Microsoft Entra ID (formerly AAD) is responsible for enforcing those permissions.  Microsoft Entra ID (formerly AAD) maintains role-based access control policies to control access between users or processes acting on behalf of users and devices, files, records, domains, and more in information systems. In addition to enforcing authorized access at the information system level and recognizing that information systems can host many applications and services in support of organizational missions and business operations, access enforcement mechanisms can also be employed at the application and service level to provide increased information security.  **Azure**  Azure enforces approved authorizations for logical access to the Azure environment using role-based access control enforced by Active Directory. Access to Active Directory security groups is managed through OneIdentity, MyAccess, and CoreIdentity. Only screened personnel can access services in the Azure environment.  All accounts created in support of Azure are role-based. Service team users request access to Azure, and if approved, are placed in the appropriate security groups according to their roles for supporting their services, using the principles of least privilege.  By default, accounts do not have persistent elevated permissions to the production environment. If an Azure user needs access to the production environment to perform a specific action, they request temporary Just in Time (JIT) access through the JIT portal. Approval is granted either automatically using preconfigured rules or a different Azure user with the access approver role. Access is only provided for a finite period based on the expected duration of the work to be performed. If access is approved, the user is assigned the minimum permissions required to perform the work, and permission is automatically revoked at the end of the specified time. |

## AC-4 Information Flow Enforcement

Enforce approved authorizations for controlling the flow of information within the system and between connected systems based on [information flow control policies within the system and between connected systems are defined;].

|  |
| --- |
| **AC-4 Control Summary Information** |
| Responsible Roles: Networking, SDN, SDL |
| Parameter ac-4: deny-all, approve-by-exception information flow policies |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AC-4 What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for controlling the flow of information within customer-deployed resources and between interconnected systems.  **Azure**  Azure enforces approved authorizations for controlling the flow of information within the system and between interconnected systems by using the following features and controls.  **VLAN Isolation**  The Azure environment is logically segregated using software Virtual Local Area Networks (VLANs) to separate customer traffic from the rest of the Azure and Microsoft networks. The Azure environment in any datacenter is logically segregated into three primary VLANs – the Universal Fabric Controller (UFC) VLAN, the Fabric Controller (FC) VLAN, and a main VLAN that houses the rest of the components including the VMs and storage. Customer data sits behind the main VLAN and is segregated from other customer’s data. A brief description of each VLAN is below:  \* UFC VLAN - Used for communication between the UFC and FCs  \* FC VLAN - Used for communication between FCs and other network devices  \* Main VLAN - Used for customer VMs and FCs  VLANs partition a network such that no communication is possible between VLANs without passing through a router. This prevents a compromised asset from faking traffic from outside its VLAN and from eavesdropping on traffic that is not to or from its VLAN. VLANs and ACLs restrict network communications by source and destination IP addresses, protocols, and port numbers. Communication is permitted from the FC VLAN to the main VLAN but cannot be initiated from the main VLAN to the FC VLAN, protecting the fabric from customers.  As the central orchestrator of much the Azure infrastructure, significant controls are in place to mitigate threats to FCs, especially from potentially compromised Azure VMs within customer applications. FCs do not recognize any hardware whose device information such as a MAC address is not pre-loaded in the FC. The DHCP servers on the FC have configured lists of MAC addresses of the assets they are willing to boot. Even if unauthorized assets are connected, they are not incorporated into the Fabric inventory. This reduces the risk of unauthorized assets communicating with the FC and gaining access to the VLAN.  **Software Load Balancers**  Access to the Azure environment from outside the cluster is restricted through Software Load Balancers (SLBs). The SLB is a networking device that accepts internet traffic coming into Azure and forwards it to an appropriate internal IP address and port within the Fabric. In the common case where there are several different machines or VMs that can handle a given request, the SLB allocates the connections in a way that balances the load among them. The SLB routing tables are updated as VMs are created, deleted, and moved from one piece of hardware to another.  **Virtual Filtering Platform (VFP) Filter**  The Virtual Filtering Platform (VFP) Filter component in the Host OS isolates the Host OS from the Guest VMs and the Guest VMs from one another. It performs filtering of traffic to restrict communication between tenant's assets and the internet based on the customer's service configuration, segregating them from other tenants. The VFP Filter component on the VM allow passage of only those packets called out in the configuration documents of those VMs.  Customers must explicitly open ports on their role instances by configuring the port number in their Service Definition file. There is no port that is open by default unless explicitly configured by the customer in the service definition. Once configured, the FC automatically updates the network traffic rule sets on VFP Filter as well as on the SLB to allow external traffic only through the designated ports.  In addition, there is a VFP Filter on each customer VM which the customer is responsible for configuring the range of IP addresses authorized to access the customer environment.  **Firewall**  For scalability and reliability in a hyperscale environment, Azure does not implement traditional firewall architecture at the perimeter between the external and Azure environments to Azure internal components, but achieves the same effect using a series of firewalls at the OS layer, including a host firewall, hypervisor firewall, and VM firewall. All infrastructure components are assigned IP addresses that are from Dedicated IPs (DIPs) allocated from non-routable address space. Therefore, an attacker on the internet cannot route traffic to those addresses as they do not reach Azure. In the unlikely event the attacker was able to route the traffic to the addresses, the Azure Gateway routers filter all packets addressed to internal addresses so they do not enter the network. The only components that accept traffic directed to Virtual IPs (VIPs) are the Azure software load balancers.  **Access Control Lists (ACLs)**  Azure only allows connections and communication which are necessary to allow services to operate, blocking all other ports, protocols and connections by default, as defined in Microsoft’s Online Services Network Security Standard. Access Control Lists (ACLs) are the preferred mechanism to restrict network communications by source and destination networks, protocols, and port numbers. Approved mechanisms to implement networked-based ACLs include: tiered ingress ACLs on routers managed by Azure Networking, IPSec policies applied to hosts to restrict communications when used in conjunction with tiered ACLs, network firewall rules, and host-based firewall rules.  Certain communications as defined in the Firewall Rule and Tiered ACL Guidelines are pre-approved and therefore permitted without requiring further review by online services security. The Firewall Rule and Tiered ACL Guidelines define the ingress and egress ACLs specifying the approved protocols and ports for each key connection point based upon the asset classification of the data. Azure requires all ACLs involving ingress and egress ports other than what is listed within the Firewall Rule and Tiered ACL Guidelines, to obtain approval through the Security Review Process prior to implementation.  **Applications**  For data flowing between application components, service teams control input by using an input validation method stipulated by Microsoft’s Security Development Lifecycle (SDL) process, further detailed in the CM and SA families of controls. Input validation testing includes regulating data inputs by size, formation, and structure prior to allowing information to reach the underlying database. The backend services and servers receive only pre-validated inputs from the front-end webservers. The backend is not directly accessible, from an application data flow perspective, in any other method. |

### AC-4(4) - Flow Control of Encrypted Information

Prevent encrypted information from bypassing [intrusion detection mechanisms] by [Selection (OneOrMore): decrypting the information;blocking the flow of the encrypted information;terminating communications sessions attempting to pass encrypted information;[the organization-defined procedure or method used to prevent encrypted information from bypassing information flow control mechanisms is defined (if selected);] ] .

Requirement: The service provider must support Agency requirements to comply with M-21-31 (https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-31-Improving-the-Federal-Governments-Investigative-and-Remediation-Capabilities-Related-to-Cybersecurity-Incidents.pdf) and M-22-09 (https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf).

|  |
| --- |
| **AC-4(4) Control Summary Information** |
| Responsible Roles: Azure Compliance |
| Parameter ac-04.04\_odp.01: Not applicable |
| Parameter ac-04.04\_odp.02: Not applicable |
| Parameter ac-04.04\_odp.03: |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☒ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☒ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AC-4(4) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for preventing encrypted information from bypassing content-checking mechanisms by (one or more): decrypting the information; blocking the flow of the encrypted information; terminating communications sessions attempting to pass encrypted information; organization-defined procedure or method.  **Azure**  Azure does not monitor or examine customer data by design. The customer is fully responsible for ensuring they can monitor and content-check their encrypted information. |

### AC-4(21) - Physical or Logical Separation of Information Flows

Separate information flows logically or physically using [Assignment: organization-defined mechanisms and/or techniques] to accomplish [required separations by types of information are defined;].

|  |
| --- |
| **AC-4(21) Control Summary Information** |
| Responsible Roles: Networking, SDN, SDL |
| Parameter ac-4.21\_prm\_1: TLS |
| Parameter ac-04.21\_odp.01: |
| Parameter ac-04.21\_odp.02: |
| Parameter ac-04.21\_odp.03: separation of all sessions |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AC-4(21) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for separating information flows within customer-deployed resources.  **Azure**  Azure logically separates information flows using ACLs. ACLs are the preferred mechanism to restrict network communications by source and destination networks, protocols, and port numbers. Approved mechanisms to implement networked-based ACLs include: tiered ACLs on routers managed by Azure Networking, IPSec policies applied to hosts to restrict communications when used in conjunction with tiered ACLs, network firewall rules, and host-based firewall rules.  Additionally, Azure separates all information flows logically using user session encryption. TLS ensures the confidentiality and integrity of each flow; only the intended recipient can decrypt information.  For data flowing between application components, service teams control input by using an input validation method stipulated by Microsoft’s Security Development Lifecycle (SDL) process, further detailed in the CM and SA families of controls. Input validation testing includes regulating data inputs by size, formation, and structure prior to allowing information to reach the underlying database. The backend services and servers receive only pre-validated inputs from the front-end webservers. The backend is not directly accessible, from an application data flow perspective, in any other method. |

## AC-5 Separation of Duties

a. Identify and document [duties of individuals requiring separation are defined;] ; and

b. Define system access authorizations to support separation of duties.

Guidance: CSPs have the option to provide a separation of duties matrix as an attachment to the SSP.

|  |
| --- |
| **AC-5 Control Summary Information** |
| Responsible Roles: JIT, OneIdentity, Network Access Control |
| Parameter ac-5(a): duties as defined in the Azure Access Control Standard Operating Procedure (SOP), the Azure Software Change and Release Management Standard Operating Procedure (SOP), and the Azure Hardware Change and Release Management Standard Operating Procedure (SOP) |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AC-5 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  The customer is responsible for identifying and documenting duties requiring separation across customer-controlled accounts.  **Azure**  Azure identifies and documents separation of duties in the Azure Access Control Standard Operating Procedure (SOP), the Azure Software Change and Release Management Standard Operating Procedure (SOP), and Azure Hardware Change and Release Management Standard Operating Procedure (SOP). Separation of duties is also enforced and documented via standard account approvals, JIT approvals, Break-Glass account incident tickets, and exception requests. |
| **Part B**  **Customer Responsibility**  The customer is responsible for defining system access authorizations to support separation of duties across customer-controlled accounts.  **Azure**  Azure enforces separation of duties within the environment through role-based security groups defined in AD, through JIT access, and through Break-Glass account alerting. Each user is a member of a certain security group or set of security groups that enforces access to the system based on the appropriate roles associated with that security group.  Azure users are assigned to security roles, which have a defined list of available permissions. By default, no accounts have active permissions to the production environment. If an Azure user needs access to the production environment to perform a specific action, they request temporary Just in Time (JIT) access through the JIT portal. Approval is granted either automatically using preconfigured rules or a different Azure user with the access approver role reviews and approves or denies the type of access requested. Access is only provided for a finite time based on the expected duration of the work to be performed. If access is approved, the user is assigned the minimum permissions required to perform the work, and permission is automatically revoked at the end of the specified time. Implementing access control using JIT access via the JIT portal effectively prevents malevolent activity without collusion, as an individual must review and approve the requestor's access request and denies requests that violate separation of duties requirements. Regardless of JIT access, reviews of accounts and all approved access occur quarterly through the Quarterly Access Review (QAR).  Break-Glass accounts have persistent administrative access, but generate Severity 2 incident tickets when accessed, ensuring that separation of duties is maintained due to the requirement to investigate each use. Exceptions to the JIT and Break-Glass account procedures are required to be approved prior to being created and utilized on the production network. This small number of accounts has persistent administrative access to the production environment but must follow all account management requirements before being approved and are monitored closely.  Azure also establishes separation of duties on critical functions within the Azure production environment to minimize the risk of unauthorized changes to production services. This is accomplished by separating the responsibilities for requesting, approving, and deploying changes to authorized Azure teams and personnel. Development and testing responsibilities for new software builds or changes to existing software are separated and managed through restricted access to branches within Git and segregated in the development and production environments. Features and changes are developed by the Azure service teams and are reviewed and tested by designated service team members for quality assurance and compatibility with the rest of the platform. |

## AC-6 Least Privilege

Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.

|  |
| --- |
| **AC-6 Control Summary Information** |
| Responsible Roles: JIT, OneIdentity, Network Access Control |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AC-6 What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for enforcing least privilege across customer-controlled accounts.  **Azure**  Privileges to Azure production services and administrative interfaces are assigned to Azure personnel based on least privilege principles in accordance with job responsibilities. Elevated access must be approved by the respective account managers.  OneIdentity, MyAccess, and CoreIdentity, used for access provisioning to resources, are based on structured business resources/rules created by the Azure service teams. They are used to grant Azure personnel membership access to designated and restricted security groups on least privilege principles. Service teams can obtain Just in Time (JIT) for troubleshooting purposes. JIT access is provided though the JIT portal based on the workflow configured and the access is granted only to the requested assets. The access can be configured to support business needs and can range from one (1) hour to twenty four (24) hours and revoked based on the JIT policy settings prescribed by the resource owner. Break-Glass accounts are provided the minimum permissions necessary to execute work if JIT is nonfunctioning.  Access to Azure services is granted based upon need-to-know and least-privilege principles. Access that has not been explicitly permitted is denied by default. Role-based access controls are used to allocate logical access to a specific job function or area of responsibility, rather than to an individual. |

### AC-6(1) - Authorize Access to Security Functions

Authorize access for [individuals and roles with authorized access to security functions and security-relevant information are defined;] to:

(a) [all functions not publicly accessible] ; and

(b) [all security-relevant information not publicly available].

|  |
| --- |
| **AC-6(1) Control Summary Information** |
| Responsible Roles: JIT, OneIdentity |
| Parameter ac-6.1\_prm\_2: Staff access is granted based on access management tools and approvals |
| Parameter ac-06.01\_odp.01: Azure resources |
| Parameter ac-06.01\_odp.02: |
| Parameter ac-06.01\_odp.03: |
| Parameter ac-06.01\_odp.04: |
| Parameter ac-06.01\_odp.05: Azure resources and data stored within |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AC-6(1) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for authorizing access to security functions and security-relevant information for customer-controlled accounts.  **Azure**  For all Azure assets, logical access is explicitly authorized. Azure requires explicit authorization before granting access to Azure, including but not limited to any of the following security functions: establishing system accounts; configuring access authorizations; authentication; setting events to be audited; and system and security administration access to log data. OneIdentity and MyAccess are used to document authorization to Azure resources based on structured business rules using designated and restricted security groups that prescribe which Azure components a user can access. |

### AC-6(2) - Non-privileged Access for Nonsecurity Functions

Require that users of system accounts (or roles) with access to [all security functions] use non-privileged accounts or roles, when accessing nonsecurity functions.

Guidance: Examples of security functions include but are not limited to: establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters, system programming, system and security administration, other privileged functions.

|  |
| --- |
| **AC-6(2) Control Summary Information** |
| Responsible Roles: JIT, OneIdentity, Network Access Control |
| Parameter ac-06.02\_odp: all security functions |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AC-6(2) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for requiring the use of non-privileged accounts/roles when accessing non-security functions for customer-deployed resources.  **Azure**  Azure personnel do not have persistent elevated access by default to the Azure production environment. Azure requires users to use their accounts for specific job functions that require the appropriate level of access needed. Elevated access is used only for those specified job functions required by the user's responsibilities; temporary elevated access is granted through JIT based on a valid business justification. Persistent elevated access in the form of Break-Glass accounts are not permitted to be used except for management and operation of the system. In addition, no unprivileged actions such as use of web browsers, email clients, etc., are allowed within the production environment. |

### AC-6(3) - Network Access to Privileged Commands

Authorize network access to [all privileged commands] only for [compelling operational needs necessitating network access to privileged commands are defined;] and document the rationale for such access in the security plan for the system.

|  |
| --- |
| **AC-6(3) Control Summary Information** |
| Responsible Roles: JIT, OneIdentity, Network Access Control |
| Parameter ac-06.03\_odp.01: all elevated commands |
| Parameter ac-06.03\_odp.02: maintenance and operational needs |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AC-6(3) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for enforcing least privilege when authorizing network access to elevated commands for customer-deployed resources, rationale for such authorizations should be documented in the system security plan (SSP).  **Azure**  Azure establishes conditions for system account group membership using Active Directory. All group membership for Azure services must be approved by the respective security group owner. Users are not granted membership to account groups for which they do not require access. Following the least privilege principle, group membership is given with the minimum access needed by the authorized individual to perform his or her job function and role.  Elevated commands can only be executed by administrative accounts, which are either compliant with JIT and Break-Glass accounts and must be authorized and approved prior to or upon use, or are exception accounts that must be approved formally to maintain persistent administrative access. |

### AC-6(5) - Privileged Accounts

Restrict privileged accounts on the system to [personnel or roles to which privileged accounts on the system are to be restricted is/are defined;].

|  |
| --- |
| **AC-6(5) Control Summary Information** |
| Responsible Roles: JIT, OneIdentity, Network Access Control |
| Parameter ac-06.05\_odp: internal Azure roles defined in AC-02 Part a |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AC-6(5) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for restricting privileged customer-controlled accounts.  **Azure**  Azure restricts elevated access via the OneIdentity groups to which a user belongs. These groups determine which assets the user is able to reach via elevated access. |

### AC-6(7) - Review of User Privileges

(a) Review [at a minimum, annually] the privileges assigned to [all users with privileges] to validate the need for such privileges; and

(b) Reassign or remove privileges, if necessary, to correctly reflect organizational mission and business needs.

|  |
| --- |
| **AC-6(7) Control Summary Information** |
| Responsible Roles: OneIdentity, Network Access Control |
| Parameter ac-06.07\_odp.01: at least annually |
| Parameter ac-06.07\_odp.02: all users |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AC-6(7) What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  The customer is responsible for reviewing user privileges of customer-controlled accounts.  **Azure**  Azure Security generates reports containing user privilege assignments to each service team at least quarterly. Service teams use this report to review user privileges for the various users and roles administering the service and validate the need for the assigned privileges. |
| **Part B**  **Customer Responsibility**  The customer is responsible for reassigning or removing privileges for customer-controlled accounts when appropriate.  **Azure**  Any user who no longer is in a role that requires access is removed as part of the review process, either by the manager identifying it as not required or due to lack of response from the manager. |

### AC-6(8) - Privilege Levels for Code Execution

Prevent the following software from executing at higher privilege levels than users executing the software: [any software except software explicitly documented].

|  |
| --- |
| **AC-6(8) Control Summary Information** |
| Responsible Roles: JIT |
| Parameter ac-06.08\_odp: any software except software explicitly documented |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AC-6(8) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for enforcing software execution privileges on customer-deployed resources.  **Azure**  Software execution at a higher privilege level than users executing the software is not possible for servers and network devices. Azure only permits administrator access to server who by default have code execution privileges. These users have full access to the system, preventing users being indirectly provided greater privileges than assigned by Microsoft. |

### AC-6(9) - Log Use of Privileged Functions

Log the execution of privileged functions.

|  |
| --- |
| **AC-6(9) Control Summary Information** |
| Responsible Roles: Logging and Monitoring |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AC-6(9) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for auditing the execution of privileged functions on customer-deployed resources.  **Azure**  Azure captures the execution of privileged functions that are useful in monitoring and investigation of elevated access. These logs are evaluated and required by the service teams and/or Security Response Team for inclusion as reasonable data for analysis. |

### AC-6(10) - Prohibit Non-privileged Users from Executing Privileged Functions

Prevent non-privileged users from executing privileged functions.

|  |
| --- |
| **AC-6(10) Control Summary Information** |
| Responsible Roles: JIT, OneIdentity, Network Access Control |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AC-6(10) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for ensuring that non-privileged users cannot execute privileged functions on customer-deployed resources.  **Azure**  Azure prevents non-privileged users from accessing elevated functions. Non-privileged service team users are never granted access to Azure. Customers do not have access to any functionality related to Azure safeguards/countermeasures. |

## AC-7 Unsuccessful Logon Attempts

a. Enforce a limit of [the number of consecutive invalid logon attempts by a user allowed during a time period is defined;] consecutive invalid logon attempts by a user during a [the time period to which the number of consecutive invalid logon attempts by a user is limited is defined;] ; and

b. Automatically [Selection (OneOrMore): lock the account or node for [time period for an account or node to be locked is defined (if selected);] ;lock the account or node until released by an administrator;delay next logon prompt per [delay algorithm for the next logon prompt is defined (if selected);] ;notify system administrator;take other [other action to be taken when the maximum number of unsuccessful attempts is exceeded is defined (if selected);] ] when the maximum number of unsuccessful attempts is exceeded.

Requirement: In alignment with NIST SP 800-63B.

|  |
| --- |
| **AC-7 Control Summary Information** |
| Responsible Roles: OneIdentity, Network Access Control, VPN, Jumpbox, MFA |
| Parameter ac-07\_odp.01: not more than five (5) |
| Parameter ac-07\_odp.02: fifteen (15) minutes |
| Parameter ac-07\_odp.03: locks the account/node until released by an administrator |
| Parameter ac-07\_odp.04: |
| Parameter ac-07\_odp.05: |
| Parameter ac-07\_odp.06: |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☒ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AC-7 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  The customer is responsible for enforcing a limit of consecutive failed login attempts on customer-deployed resources.  **Azure**  For all access to the environment, Azure personnel must use multifactor authentication using a smart card and PIN. smart card authentication enforces lockout after five (5) failed login attempts. After five (5) invalid access attempts within fifteen (15) minutes, a user’s smart card is locked out until it is unblocked by an administrator. The smart card is tied to the user’s Microsoft Entra ID (formerly AAD)account, using the CorpNet-alias-derived unique identifier for the environment, which is used for access throughout Azure via single-sign-on. Local account settings inherit the smart card settings, ensuring that after five invalid PIN entries, the user’s smart card is locked, rather than any accounts they may be logging into – ensuring that their access remains locked until their smart card is unlocked by an administrator. |
| **Part B**  **Customer Responsibility**  The customer is responsible for taking action when a user has reached the number of failed login attempts within the time period documented in AC-07 Part a.  **Azure**  For all access to the environment, Azure personnel must use multifactor authentication using a smart card and PIN. Once a user’s smart card is locked out after five (5) invalid access attempts against the smart card, the user must contact an administrator through the help desk to manually unblock and reset the PIN. |

## AC-8 System Use Notification

a. Display [see additional Requirements and Guidance] to users before granting access to the system that provides privacy and security notices consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and state that:

1. Users are accessing a U.S. Government system;

2. System usage may be monitored, recorded, and subject to audit;

3. Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and

4. Use of the system indicates consent to monitoring and recording;

b. Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system; and

c. For publicly accessible systems:

1. Display system use information [see additional Requirements and Guidance] , before granting further access to the publicly accessible system;

2. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and

3. Include a description of the authorized uses of the system.

Requirement: The service provider shall determine elements of the cloud environment that require the System Use Notification control. The elements of the cloud environment that require System Use Notification are approved and accepted by the JAB/AO.

Requirement: The service provider shall determine how System Use Notification is going to be verified and provide appropriate periodicity of the check. The System Use Notification verification and periodicity are approved and accepted by the JAB/AO.

Requirement: If not performed as part of a Configuration Baseline check, then there must be documented agreement on how to provide results of verification and the necessary periodicity of the verification by the service provider. The documented agreement on how to provide verification of the results are approved and accepted by the JAB/AO.

Guidance: If performed as part of a Configuration Baseline check, then the % of items requiring setting that are checked and that pass (or fail) check can be provided.

|  |
| --- |
| **AC-8 Control Summary Information** |
| Responsible Roles: JIT, OneIdentity, Network Access Control, VPN, Jumpbox |
| Parameter ac-08\_odp.01: a system use notification specified in Part a below |
| Parameter ac-08\_odp.02: Not applicable |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AC-8 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  The customer is responsible for implementing a compliant system use notification for all customer-deployed resources.  **Azure**  All access methods into the Azure production environment include a warning banner prior to administrative login to all servers and network devices. There are two approved messages reviewed by Microsoft Corporate, External, and Legal Affairs (CELA). The first states:  "You are accessing an information system that may contain U.S. Government data. System usage may be monitored, recorded, and subject to audit. Unauthorized use of the system is prohibited and may be subject to criminal and civil penalties. Use of the system indicates consent to monitoring and recording. Administrative personnel remotely accessing the Azure environment:  \* Maintain their remote computer in a secure manner, in accordance with organizational security policies and procedures as defined in the Network Security Standard.  \* Only access the Azure environment in execution of operational, deployment, and support responsibilities using only administrative applications or tools directly related to performing these responsibilities.  \* Are advised to not knowingly store, transfer into, or process in the Azure environment data exceeding a Federal Information Processing Standards (FIPS) 199 High security categorization (FISMA Controlled Unclassified Information)."  An alternate approved wording states:  "You are accessing an information system that may contain U.S. Government data. System usage may be monitored, recorded, and subject to audit. Unauthorized use of the system is prohibited and may be subject to criminal and civil penalties. Use of the system indicates consent to monitoring and recording. Administrative personnel remotely accessing the Azure environment:  (1) shall maintain their remote computer in a secure manner, in accordance with organizational security policies and procedures as defined in the Network Security Standard;  (2) shall only access the Azure environment in execution of operational, deployment, and support responsibilities using only administrative applications or tools directly related to performing these responsibilities; and  (3) shall not knowingly store, transfer into, or process in the Azure environment data exceeding a Federal Information Processing Standards (FIPS) 199 Moderate security categorization (FISMA Controlled Unclassified Information)."  A warning message is also presented to users requesting JIT elevation at the JIT access portal, prior to obtaining elevated permissions. This message states that the user is accessing an information system that may contain sensitive data; that system usage may be monitored, recorded, and subject to audit; and that unauthorized use of the system is prohibited and may be subject to criminal and civil penalties. |
| **Part B**  **Customer Responsibility**  The customer is responsible for requiring users to acknowledge the system use notification described in AC-08 Part a on customer-deployed resources.  **Azure**  The warning banner is displayed during the logon sequence. Microsoft users must take explicit action to complete the login sequence. |
| **Part C**  **Customer Responsibility**  The customer is responsible for displaying a system use notification on all publicly accessible customer-deployed resources. The notification must include (if any) descriptions of monitoring, recording, or auditing that may be configured, and the description of authorized uses of the system.  **Azure**  Azure does not display a warning banner on customer interfaces. Based on review of requirements and discussions with Azure environment service owners, this control is not applicable to the customer-facing components of the Azure environment as Azure is a commercial service and customers are responsible for implementing this control either at the proxy level, the application/client level, or on their ADFS server that authenticates their users who access the Azure environment. |

## AC-10 Concurrent Session Control

Limit the number of concurrent sessions for each [accounts and/or account types for which to limit the number of concurrent sessions is defined;] to [three (3) sessions for privileged access and two (2) sessions for non-privileged access].

|  |
| --- |
| **AC-10 Control Summary Information** |
| Responsible Roles: JIT, Networking, SDL, VPN, Jumpbox |
| Parameter ac-10\_odp.01: all accounts and account types |
| Parameter ac-10\_odp.02: unlimited concurrent sessions |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☒ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AC-10 What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for defining and enforcing the limit of concurrent sessions for each customer-controlled account and/or account type.  **Azure**  **Servers**  Azure does not currently limit the number of concurrent sessions to production operating systems. However, users can only log in via Remote Desktop Protocol (RDP) once with their credentials. This limits sessions to one session per host, per user. Additionally, the following compensating access control measures are in place: multifactor authentication is required for all access to Azure services for Azure personnel; account lockout is enforced for invalid login attempts at the smart card level; access to administrative interfaces is limited to approved access through role-based access control, ensuring that the risk of exploit by other than specifically designated personnel is low to non-existent.  Conversely, prohibiting concurrent sessions would hinder Azure administration and maintenance. Azure requires specialized, non-public software tools and utilities. These create dedicated sessions directly associated with the tool. Trouble investigation such as running diagnostics require multiple instances of these tools, often for extended periods.  **Network Devices**  Accessing network devices in the Azure environment requires users to establish a connection to the Azure Network Hop Boxes or to connect to the VPN before connecting to the Azure environment. When establishing a connection to a network device, a user must authenticate with a physical Azure-issued smart card before establishing a session to an Azure domain server. The multifactor authentication provided by the physical smart card and PIN combination requirement provides additional security when access to network devices is attempted. Concurrent sessions are implemented at the Azure Network Hop Boxes or to connect to the VPN for the network devices versus at the individual device layer.  **Software**  Service team web applications enforce a limit of one session per browser cookie for all customer user sessions. |

## AC-11 Device Lock

a. Prevent further access to the system by [Selection (OneOrMore): initiating a device lock after [fifteen (15) minutes] of inactivity;requiring the user to initiate a device lock before leaving the system unattended] ; and

b. Retain the device lock until the user reestablishes access using established identification and authentication procedures.

|  |
| --- |
| **AC-11 Control Summary Information** |
| Responsible Roles: Corporate IT, Jumpbox, PAW |
| Parameter ac-11\_odp.01: Corp workstation at fifteen (15) minutes, SAW at ten (10) minutes, Pule Secure VPN at sixty (60) minutes |
| Parameter ac-11\_odp.02: |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AC-11 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  The customer is responsible for preventing further access to the system by initiating a device lock after an organization-defined time period of inactivity or requiring the user to initiate a device lock before leaving the system unattended.  **Azure**  Core Services Engineering and Operations (CSEO) is responsible for corporate domain settings that enforce a session lock of at most fifteen (15) minutes on Corporate Network (CorpNet) workstations. Secure Admin Workstations (SAWs) have session lock settings of ten (10) minutes. Access to Azure is only possible from Core Services Engineering and Operations (CSEO)-issued SAWs. All access requires the user to utilize a SAW, unless there is a Break-Glass scenario, in which case the CorpNet workstation is used. In addition to the SAW or CorpNet workstations, pulse secure VPN connection is utilized to access production assets. The pulse secure VPN is configured to conduct session lock after 60 minutes of inactivity. |
| **Part B**  **Customer Responsibility**  The customer is responsible for retaining the device lock until the user reestablishes access using established identification and authentication procedures on customer-deployed resources.  **Azure**  The only way for the user to end the session lock is by reestablishing access using their credentials on their CorpNet workstation or SAW and pulse secure VPN. |

### AC-11(1) - Pattern-hiding Displays

Conceal, via the device lock, information previously visible on the display with a publicly viewable image.

|  |
| --- |
| **AC-11(1) Control Summary Information** |
| Responsible Roles: Corporate IT, Jumpbox, PAW |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AC-11(1) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for concealing previously-visible information when a session lock is initiated on customer-deployed resources.  **Azure**  The Windows operating system running on the Secure Admin Workstation (SAW) performs lock functionality and displays blank login screen when a session is locked. |

## AC-12 Session Termination

Automatically terminate a user session after [conditions or trigger events requiring session disconnect are defined;].

|  |
| --- |
| **AC-12 Control Summary Information** |
| Responsible Roles: JIT, OneIdentity, Network Access Control, VPN, Jumpbox |
| Parameter ac-12: a logout request initiated by user for customers; a logout request initiated by user or 15 minutes of inactivity by Azure personnel |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AC-12 What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for defining and enforcing events or conditions requiring the termination of a user session on customer-deployed resources.  **Azure**  Azure automatically terminates Microsoft user sessions upon receiving a logout request from the user. Secure Admin Workstations (SAWs) require re-authentication after at most ten (10) minutes of user inactivity.  **VPN**  The SAW VPN terminates inactive sessions after ten (10) minutes of inactivity, and the non-SAW VPN terminates inactive sessions after sixty (60) minutes of inactivity.  **Servers**  RDP and SSH idle timeout inherit the settings of the target server. Azure servers are configured to terminate idle sessions after fifteen (15) minutes of inactivity.  **Network Devices**  SSH idle timeout inherits the settings of the target network device. Azure network devices are configured to terminate inactive sessions after sixty (60) minutes. |

## AC-14 Permitted Actions Without Identification or Authentication

a. Identify [user actions that can be performed on the system without identification or authentication are defined;] that can be performed on the system without identification or authentication consistent with organizational mission and business functions; and

b. Document and provide supporting rationale in the security plan for the system, user actions not requiring identification or authentication.

|  |
| --- |
| **AC-14 Control Summary Information** |
| Responsible Roles: Azure Compliance, Microsoft Entra ID (formerly AAD) |
| Parameter ac-14(a): Not applicable for Microsoft personnel, only the login page and limited public information is accessible for external users without authentication |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AC-14 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  The customer is responsible for identifying actions that can be performed on the customer-deployed resources without identification or authentication, such as viewing a publicly accessible web page designed and configured by the customers. Customers can build rich sites, applications, and services using Azure. Those customer-developed sites, applications, and services must have authorization enforced using the ADFS authentication provided by the customer.  **Azure**  The only actions permitted by Azure to be performed without identification and authentication are accessing the public Feature Descriptions, Developer Documents, Legal, Privacy Statement, Help, and Language Preference options on the customer facing welcome page. On the welcome page the user enters his or her email address, at which point Active Directory Federation Services (ADFS) refers the user back to the customer-controlled federated authentication portal.  Service teams also make aspects of their services consumable as needed. For instance, Microsoft Entra ID (formerly AAD) DNS responds to unauthenticated DNS queries by design, as this is required to be compliant with the DNS specification and to ensure customers can successfully resolve Microsoft Entra ID (formerly AAD) URLs. |
| **Part B**  **Customer Responsibility**  The customer is responsible for providing documentation for user actions not requiring identification or authentication on customer-deployed resources. It is the responsibility of the customer to follow their own Rules of Behavior and policies around inviting guests to customer managed resources.  **Azure**  The information in the Feature Descriptions, Developer Documents, Legal, Privacy Statement, Help, and Language Preference is either legally required or foundational to an internet-facing service and none of it impacts the security of the system if disclosed. Service teams also make aspects of their services consumable as needed. For instance, Microsoft Entra ID (formerly AAD) DNS responds to unauthenticated DNS queries by design, as this is required to be compliant with the DNS specification and to ensure customers can successfully resolve Microsoft Entra ID (formerly AAD) URLs. |

## AC-17 Remote Access

a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and

b. Authorize each type of remote access to the system prior to allowing such connections.

|  |
| --- |
| **AC-17 Control Summary Information** |
| Responsible Roles: JIT, OneIdentity, Network Access Control, VPN, Jumpbox |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AC-17 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  The customer is responsible for establishing and documenting remote access requirements to customer-deployed resources, including usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed.  **Azure**  There are several authentication steps to be able to access Azure resources remotely. Authorized Microsoft personnel utilize Microsoft-issued Secure Admin Workstations (SAWs) and connect remotely to Azure from the Corporate Network (CorpNet). Microsoft internal user connections originate in CorpNet passing via the CorpNet Firewall through Azure-managed load balancers. Users are identified by a unique Active Directory (AD) identifier on CorpNet with multifactor authentication. If a user is not at a physical Microsoft location, remote access to CorpNet also requires corporate MSFTVPN connectivity using Microsoft-issued smart card certificates and PIN-based authentication.  Once authenticated through CorpNet, Microsoft personnel access the Azure environment in one of two ways – via the VPN or via the Jumpbox, Debug Server, and Network Hop Box infrastructure. The VPN provides direct access via RDP and SSH to the assets. Alternatively, personnel can log into Jumpboxes and Debug servers for server access and Network Hop Boxes for network device access. Once through the VPN, Jumpbox, Debug Server, or Network Hop Box, the user can access Azure assets.  **Jumpboxes and Debug Servers**  Jumpboxes are servers in Azure datacenters that provide remote access paths into the Azure production environment. Azure users log into these Jumpboxes to perform routine maintenance, emergency repairs, diagnosis, and administration of Azure production environment. Access to the Jumpboxes via RDP is restricted to CorpNet and requires multifactor authentication using the user's AD credential and a smart card. Access to Jumpboxes is restricted to designated OneIdentity security groups.  Similar to Jumpboxes, Debug servers are non-domain-joined servers located entirely within the Azure production environment. users connect to Debug servers via RDP using specific, CorpNet-exposed endpoints before accessing Azure assets. Access to Debug servers is similarly restricted to designated OneIdentity security groups.  **Network Hop Boxes**  Network Hop Boxes are the network device equivalent of the server Jumpboxes for Azure network devices.  **VPN**  Personnel utilize the following methods via SSL VPN to access Azure production assets:  \* Public Key Infrastructure (PKI) to enable secure communication between the certificate server to the target asset by utilizing CRL Validation  \* Leveraging Microsoft Entra ID (formerly AAD) through utilization of multifactor authentication via smart card from the identity server to the target asset |
| **Part B**  **Customer Responsibility**  The customer is responsible for authorizing each type of remote access to the system prior to allowing such connections.  **Azure**  Azure authorizes remote access for Azure service team users. Before service team personnel can connect to Azure remotely, they must first be approved for remote access by an authorized manager. This process is automatically enforced by OneIdentity. |

### AC-17(1) - Monitoring and Control

Employ automated mechanisms to monitor and control remote access methods.

|  |
| --- |
| **AC-17(1) Control Summary Information** |
| Responsible Roles: Logging and Monitoring |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AC-17(1) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for employing automated mechanisms for monitoring and controlling remote access methods for customer-deployed resources.  **Azure**  Azure utilizes Azure Security Monitoring (ASM) and SCUBA for monitoring logs for unauthorized remote access to the information system. ASM and SCUBA look for indicators of attempted security attacks and indicators of compromised servers. In addition, ASM and SCUBA look for indicators of attempted security attacks and indicators of compromised systems. Any unauthorized or otherwise unusual remote access to the information system automatically generates an Incident Management (IcM) ticket to the service owners or the Security Response Team for investigation. Geneva Monitoring is configured to collect remote access events from the Windows Event log. These events are uploaded to the security information and event management tools. These events are processed by the Security Response Team to ensure normal usage of the system, and to examine deviations from this range. Unusual activity is flagged for further review. |

### AC-17(2) - Protection of Confidentiality and Integrity Using Encryption

Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

|  |
| --- |
| **AC-17(2) Control Summary Information** |
| Responsible Roles: OneIdentity, VPN |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AC-17(2) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for implementing cryptographic mechanisms (e.g., TLS) to protect remote access sessions to customer-deployed resources.  **Azure**  For all asset types, Azure uses cryptographic controls to protect the confidentiality, authenticity and integrity of sensitive data while in transit or at rest. To ensure confidentiality, Azure uses both symmetric and asymmetric keys for encrypting sensitive data to prevent access from unauthorized parties. For example, secrets such as the Storage Key are encrypted using the receiving component’s public key prior to transmission. As part of the component’s deployment, the private key is installed into the runtime environment by leveraging the Azure Certificate Store (WACS) functionality provided by the Fabric. The component uses the private key installed into the WACS to decrypt the secret.  To ensure integrity, Azure uses asymmetric keys to protect unauthorized modification to sensitive data during transmission across components. For example, a component might generate a file then compute a cryptographic checksum over that file’s contents, then sign that checksum via its private key. Upon subsequent access of that file, the component first validates that the file’s contents had not been modified by recomputing the checksum over the current file contents then verifying the signature, which only requires the public key.  Azure uses Federal Information Processing Standards (FIPS) 140-2 validated cryptography for access. Azure Remote Desktop Protocol (RDP) and SSL VPN services are configured to use Federal Information Processing Standards (FIPS) 140-2 validated TLS 1.2/1.3 encryption for access. Encryption is required for all connections. PKI certificates are utilized within Azure on the internal RD gateways and are obtained through the Azure PKI, and SSL certificates utilized by access solutions. |

### AC-17(3) - Managed Access Control Points

Route remote accesses through authorized and managed network access control points.

|  |
| --- |
| **AC-17(3) Control Summary Information** |
| Responsible Roles: VPN, Jumpbox |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AC-17(3) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for routing remote access connections to customer-deployed resources through managed network access control points.  **Azure**  Azure leverages AD to control access to Azure assets. Azure is protected using Microsoft-controlled AD security groups and requires multifactor authentication via smart cards at security boundaries, including at the VPN, Jumpboxes, Debug Servers, and Network Hop Boxes. |

### AC-17(4) - Privileged Commands and Access

(a) Authorize the execution of privileged commands and access to security-relevant information via remote access only in a format that provides assessable evidence and for the following needs: [Assignment: organization-defined needs] ; and

(b) Document the rationale for remote access in the security plan for the system.

|  |
| --- |
| **AC-17(4) Control Summary Information** |
| Responsible Roles: Azure Compliance |
| Parameter ac-17.4\_prm\_1: support for operating the system |
| Parameter ac-17.04\_odp.01: |
| Parameter ac-17.04\_odp.02: |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AC-17(4) What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  The customer is responsible for authorizing privileged commands and access to security-relevant information via remote access for customer-deployed resources.  **Azure**  Azure implements Role-Based Access Control (RBAC) where access is only granted based on legitimate job responsibilities for remote access. Authorized managers approve elevated access to production assets. For elevated remote access, all personnel must use JIT when interactive elevated access is required in the Azure production environment. Except in the case of an approved exception as described below, there is no standing or persistent elevated remote access to the Azure production environment. The primary exception is Break-Glass elevated access, described below.  In scenarios where JIT does not yet support management of elevated access, standing access may exist; these gaps in JIT support are identified and tracked as an exception, which requires approval. Software deployment via automated means (i.e., not using an interactive login) does not require interactive login to a resource that is accessed via JIT. In this case, a service team member submits a job (e.g., Pull Request in Azure DevOps), and another team member reviews, approves, and then the safe deployment system deploys.  Azure maintains Break-Glass accounts with elevated access for use in the scenario that the JIT service is not available. These accounts have persistent elevated access to perform maintenance activities if JIT is unable to provide temporary elevated access. These accounts are carefully managed, only to be used in emergencies, and have notifications associated with their use. Whenever such an account is utilized, a Severity 2 incident ticket is generated that requires the service that owns the resource to investigate and determine whether the access is valid.  Because Azure support personnel do not have physical access to the datacenters, there is a business requirement for those personnel to have remote access to conduct their work on the geographically-dispersed Azure assets. Physical access to Azure datacenters is managed by Datacenter Access Tool (DCAT). Personnel that have physical access to datacenters via DCAT system are forbidden from logging in to Azure cloud environments via remote access from the datacenters. As such, physical and remote access are separated. |
| **Part B**  **Customer Responsibility**  The customer is responsible for documenting the rationale for executing privileged commands via remote access for customer-deployed resources. Rationale for such privileged command execution should be documented in the system security plan (SSP).  **Azure**  Azure implements Role-Based Access Control (RBAC) where access is only granted based on legitimate job responsibilities for remote access. Authorized managers approve elevated access to production assets. For elevated remote access, all personnel must use JIT when interactive elevated access is required in the Azure production environment. Except in the case of an approved exception as described below, there is no standing or persistent elevated remote access to the Azure production environment. The primary exception is Break-Glass elevated access, described below.  In scenarios where JIT does not yet support management of elevated access, standing access may exist; these gaps in JIT support are identified and tracked as an exception, which requires approval. Software deployment via automated means (i.e., not using an interactive login) does not require interactive login to a resource that is accessed via JIT. In this case, a service team member submits a job (e.g., Pull Request in Azure DevOps), and another team member reviews, approves, and then the safe deployment system deploys.  Azure maintains Break-Glass accounts with elevated access for use in the scenario that the JIT service is not available. These accounts have persistent elevated access to perform maintenance activities if JIT is unable to provide temporary elevated access. These accounts are carefully managed, only to be used in emergencies, and have notifications associated with their use. Whenever such an account is utilized, a Severity 2 incident ticket is generated that requires the service that owns the resource to investigate and determine whether the access is valid.  Because Azure support personnel do not have physical access to the datacenters, there is a business requirement for those personnel to have remote access to conduct their work on the geographically-dispersed Azure assets. Physical access to Azure datacenters is managed by Datacenter Access Tool (DCAT). Personnel that have physical access to datacenters via DCAT system are forbidden from logging in to Azure cloud environments via remote access from the datacenters. As such, physical and remote access are separated. |

## AC-18 Wireless Access

a. Establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access; and

b. Authorize each type of wireless access to the system prior to allowing such connections.

|  |
| --- |
| **AC-18 Control Summary Information** |
| Responsible Roles: Asset Management, Datacenter Hosting |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☒ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☒ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AC-18 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  The customer is responsible for wireless within their environment.  **Azure**  Wireless access is not permitted within the Azure environment. While wireless exists within CorpNet to allow Secure Admin Workstations (SAWs) to connect to CorpNet wirelessly, upon authentication to the Azure environment, all network connectivity for the Azure environment is through cabling, and assets do not have wireless technology internally embedded. CorpNet SAWs are outside the Azure authorization boundary. |
| **Part B**  **Customer Responsibility**  The customer is responsible for wireless within their environment.  **Azure**  Azure regularly scans for rogue wireless signals on a quarterly basis within the Azure datacenters. Results are logged and documented by the Security Response Team. Any rogue signals are investigated and removed. Azure has implemented a solution to continuously monitor and alarm on detection of rogue wireless signals. This system has been deployed to Azure authorization boundary Azure datacenters in a phased deployment. This system allows for wireless scan data to be monitored continuously by the Azure Security Incident and Event Monitoring tool. |

### AC-18(1) - Authentication and Encryption

Protect wireless access to the system using authentication of [Selection (OneOrMore): users;devices] and encryption.

|  |
| --- |
| **AC-18(1) Control Summary Information** |
| Responsible Roles: Asset Management, Datacenter Hosting |
| Parameter ac-18.01\_odp: Not applicable |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☒ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☒ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AC-18(1) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for wireless within their environment.  **Azure**  Wireless access is not permitted within the Azure environment. While wireless exists within CorpNet to allow Secure Admin Workstations (SAWs) to connect to CorpNet wirelessly, upon authentication to the Azure environment, all network connectivity for the Azure environment is through cabling, and assets do not have wireless technology internally embedded. CorpNet SAWs are outside the Azure authorization boundary. |

### AC-18(3) - Disable Wireless Networking

Disable, when not intended for use, wireless networking capabilities embedded within system components prior to issuance and deployment.

|  |
| --- |
| **AC-18(3) Control Summary Information** |
| Responsible Roles: Asset Management, Datacenter Hosting |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☒ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☒ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AC-18(3) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for wireless within their environment.  **Azure**  Wireless access is not permitted within the Azure environment. While wireless exists within CorpNet to allow Secure Admin Workstations (SAWs) to connect to CorpNet wirelessly, upon authentication to the Azure environment, all network connectivity for the Azure environment is through cabling, and assets do not have wireless technology internally embedded. CorpNet SAWs are outside the Azure authorization boundary. |

### AC-18(4) - Restrict Configurations by Users

Identify and explicitly authorize users allowed to independently configure wireless networking capabilities.

|  |
| --- |
| **AC-18(4) Control Summary Information** |
| Responsible Roles: Asset Management, Datacenter Hosting |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☒ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☒ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AC-18(4) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for wireless within their environment.  **Azure**  Wireless access is not permitted within the Azure environment. While wireless exists within CorpNet to allow Secure Admin Workstations (SAWs) to connect to CorpNet wirelessly, upon authentication to the Azure environment, all network connectivity for the Azure environment is through cabling, and assets do not have wireless technology internally embedded. CorpNet SAWs are outside the Azure authorization boundary. |

### AC-18(5) - Antennas and Transmission Power Levels

Select radio antennas and calibrate transmission power levels to reduce the probability that signals from wireless access points can be received outside of organization-controlled boundaries.

|  |
| --- |
| **AC-18(5) Control Summary Information** |
| Responsible Roles: Asset Management, Datacenter Hosting |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☒ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☒ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AC-18(5) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for wireless within their environment.  **Azure**  Wireless access is not permitted within the Azure environment. While wireless exists within CorpNet to allow Secure Admin Workstations (SAWs) to connect to CorpNet wirelessly, upon authentication to the Azure environment, all network connectivity for the Azure environment is through cabling, and assets do not have wireless technology internally embedded. CorpNet SAWs are outside the Azure authorization boundary. |

## AC-19 Access Control for Mobile Devices

a. Establish configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, to include when such devices are outside of controlled areas; and

b. Authorize the connection of mobile devices to organizational systems.

|  |
| --- |
| **AC-19 Control Summary Information** |
| Responsible Roles: Asset Management, Datacenter Hosting |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AC-19 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  All customers are responsible for establishing usage restrictions, configuration and connection requirements, and implementation guidance for organization-controlled mobile devices used to connect to Azure.  **Azure**  Unauthorized mobile computing devices are not permitted in, or directly attached to, any Azure production environment. |
| **Part B**  **Customer Responsibility**  All customers are responsible for establishing usage restrictions, configuration and connection requirements, and implementation guidance for organization-controlled mobile devices used to connect to Azure.  **Azure**  Mobile computing and data recording devices are not to be used in any of Microsoft’s production environments without prior approval by the Datacenter Management Team via an access request. Azure monitors for all unauthorized use of mobile devices in the Azure environment and performs investigations accordingly. Azure uses various colored sticker system to identify authorized devices. Monitoring of unauthorized connections of mobile devices to servers is implemented by security officers that observe that all mobile devices used on servers must have corresponding entries in the DCAT system, which captures authorization for an individual to bring in a mobile device to the datacenter. |

### AC-19(5) - Full Device or Container-based Encryption

Employ [Selection: full-device encryption;container-based encryption] to protect the confidentiality and integrity of information on [mobile devices on which to employ encryption are defined;].

|  |
| --- |
| **AC-19(5) Control Summary Information** |
| Responsible Roles: Asset Management, Datacenter Hosting |
| Parameter ac-19.05\_odp.01: Not applicable |
| Parameter ac-19.05\_odp.02: Not applicable |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☒ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AC-19(5) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for mobile devices within their environment.  **Azure**  Vendor laptops are authorized by Datacenter Management to be connected to the Azure production environment for maintenance purposes only to synthesize diagnostic information of the environment. Vendor laptops do not have logical access (i.e. credentials) to the production environment. |

## AC-20 Use of External Systems

a. [Selection (OneOrMore): establish [terms and conditions consistent with the trust relationships established with other organizations owning, operating, and/or maintaining external systems are defined (if selected);] ;identify [controls asserted to be implemented on external systems consistent with the trust relationships established with other organizations owning, operating, and/or maintaining external systems are defined (if selected);] ] , consistent with the trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to:

1. Access the system from external systems; and

2. Process, store, or transmit organization-controlled information using external systems; or

b. Prohibit the use of [types of external systems prohibited from use are defined;].

Guidance: The interrelated controls of AC-20, CA-3, and SA-9 should be differentiated as follows: AC-20 describes system access to and from external systems. CA-3 describes documentation of an agreement between the respective system owners when data is exchanged between the CSO and an external system. SA-9 describes the responsibilities of external system owners. These responsibilities would typically be captured in the agreement required by CA-3.

|  |
| --- |
| **AC-20 Control Summary Information** |
| Responsible Roles: Azure Compliance |
| Parameter ac-20\_odp.01: Not applicable |
| Parameter ac-20\_odp.02: |
| Parameter ac-20\_odp.03: |
| Parameter ac-20\_odp.04: Not applicable |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☒ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☒ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AC-20 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  The customer is responsible for establishing terms and conditions allowing authorized individuals to access the customer-deployed resources from external information systems.  **Azure**  All groups supporting Azure utilize Secure Admin Workstations (SAWs). No administrative access to the information system is allowed other than through Microsoft systems and networks. Azure does not depend on external network access, internet or otherwise, for access to the cloud. |
| **Part B**  **Customer Responsibility**  The customer is responsible for establishing terms and conditions allowing authorized individuals to process, store, or transmit customer-controlled information using external information systems.  **Azure**  No administrative access to the information system is allowed other than through Microsoft systems and networks. Azure does not depend on external network access, internet or otherwise, for access to the cloud. |

### AC-20(1) - Limits on Authorized Use

Permit authorized individuals to use an external system to access the system or to process, store, or transmit organization-controlled information only after:

(a) Verification of the implementation of controls on the external system as specified in the organization's security and privacy policies and security and privacy plans; or

(b) Retention of approved system connection or processing agreements with the organizational entity hosting the external system.

|  |
| --- |
| **AC-20(1) Control Summary Information** |
| Responsible Roles: Azure Compliance |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☒ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☒ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AC-20(1) What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  The customer is responsible for establishing terms and conditions for external systems accessing, processing, storing, or transmitting organization-defined information from customer-deployed resources.  **Azure**  No administrative access is allowed to the information system other than through Microsoft systems and networks. |
| **Part B**  **Customer Responsibility**  The customer is responsible for establishing terms and conditions for external systems accessing, processing, storing, or transmitting organization-defined information from customer-deployed resources.  **Azure**  No administrative access is allowed to the information system other than through Microsoft systems and networks. |

### AC-20(2) - Portable Storage Devices - Restricted Use

Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems using [restrictions on the use of organization-controlled portable storage devices by authorized individuals on external systems are defined;].

|  |
| --- |
| **AC-20(2) Control Summary Information** |
| Responsible Roles: Azure Compliance |
| Parameter ac-20.02\_odp: Not applicable |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☒ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☒ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AC-20(2) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for establishing terms and conditions for external systems accessing, processing, storing, or transmitting organization-defined information from customer-deployed resources.  **Azure**  No administrative access is allowed to the information system other than through Microsoft systems and networks. |

## AC-21 Information Sharing

a. Enable authorized users to determine whether access authorizations assigned to a sharing partner match the information's access and use restrictions for [information-sharing circumstances where user discretion is required to determine whether access authorizations assigned to a sharing partner match the information's access and use restrictions are defined;] ; and

b. Employ [automated mechanisms or manual processes that assist users in making information-sharing and collaboration decisions are defined;] to assist users in making information sharing and collaboration decisions.

|  |
| --- |
| **AC-21 Control Summary Information** |
| Responsible Roles: Azure Compliance |
| Parameter ac-21\_odp.01: Not applicable |
| Parameter ac-21\_odp.02: Not applicable |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☒ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☒ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AC-21 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  The customer is responsible for determining when authorized users are required to use discretion as to whether to share customer-controlled information.  **Azure**  Per Microsoft corporate and Azure security policies, Azure personnel are not authorized to share Azure data or customer content outside the security boundary and thus do not make discretionary sharing decisions. Unless approved by the customer, Azure personnel do not have access to unencrypted customer data or resources.  <https://www.microsoft.com/en-us/trust-center/privacy/customer-data-definitions> |
| **Part B**  **Customer Responsibility**  The customer is responsible for employing a process to assist users with making information sharing decisions.  **Azure**  Per Microsoft corporate and Azure security policies, Azure personnel are not authorized to share Azure data or customer content outside the security boundary and thus do not make discretionary sharing decisions. Unless approved by the customer, Azure personnel do not have access to unencrypted customer data or resources.  <https://www.microsoft.com/en-us/trust-center/privacy/customer-data-definitions> |

## AC-22 Publicly Accessible Content

a. Designate individuals authorized to make information publicly accessible;

b. Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information;

c. Review the proposed content of information prior to posting onto the publicly accessible system to ensure that nonpublic information is not included; and

d. Review the content on the publicly accessible system for nonpublic information [at least quarterly] and remove such information, if discovered.

|  |
| --- |
| **AC-22 Control Summary Information** |
| Responsible Roles: Publicly Accessible Content |
| Parameter ac-22(d): at least quarterly |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AC-22 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  The customer is responsible for designating authorized personnel to post publicly accessible information on customer-deployed resources.  **Azure**  Azure does not have any publicly accessible internal services. The only information accessible by customers are the Feature Descriptions, Developer Documents, Legal, Privacy Statement, Help, and Language Preference options on the customer facing welcome page. Azure has designated the Microsoft Content Management Team as the group authorized to make changes to this limited information. In addition to the Content Management Team, there are select, authorized individuals from within Azure that are permitted to post blog entries about Azure. |
| **Part B**  **Customer Responsibility**  The customer is responsible for training the personnel defined in AC-21 Part a to prevent disclosure of nonpublic customer-controlled information.  **Azure**  All Azure personnel, including those who maintain or produce publicly available content, are required to take Standards of Business Conduct (SBC) training. The training provides information intended to raise awareness in the areas of anti-trust, corruption, unauthorized entry/theft, business policy, public disclosure, and applicable laws and regulations. This training is required during orientation and annually thereafter. |
| **Part C**  **Customer Responsibility**  The customer is responsible for reviewing proposed content of customer-controlled information prior to posting publicly to ensure nonpublic information is not included.  **Azure**  All information must go through the Microsoft Content Management Team for review prior to being posted to ensure that nonpublic information is not made available. This review occurs as part of the normal change management processes. |
| **Part D**  **Customer Responsibility**  The customer is responsible for periodically reviewing publicly available customer-controlled content for nonpublic information.  **Azure**  The Marketing Communications team leverages an automated tool to measure volume and sentiment for social conversations around products, events, announcements, and crises. The automated tool gathers data using a number of different methods, including web crawlers, through direct relationships, and through various Application Programming Interfaces (APIs). The tool actively collects Microsoft mentions across Twitter, news sites, forums, blogs, and general public sites. The automated tool provides alerts to the Marketing Communications team based on configuration. On a monthly cadence, the Marketing Communications team prepares a Cloud Blog and Social Cloud Marketing report to manage ecosystem performance, workload performance, followers, posts, and engagements across different platforms. If any nonpublic information is identified with the automated tool alerts and in the process of producing the Cloud Blog and Social Marketing report, the Azure incident response process is followed through crisis communications to investigate and remediate the issue. |

# Awareness and Training (AT)

## AT-1 Policy and Procedures

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (OneOrMore): organization-level;mission/business process-level;system-level] awareness and training policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the awareness and training policy and the associated awareness and training controls;

b. Designate an [an official to manage the awareness and training policy and procedures is defined;] to manage the development, documentation, and dissemination of the awareness and training policy and procedures; and

c. Review and update the current awareness and training:

1. Policy [at least annually] and following [events that would require the current awareness and training policy to be reviewed and updated are defined;] ; and

2. Procedures [at least annually] and following [significant changes].

|  |
| --- |
| **AT-1 Control Summary Information** |
| Responsible Roles: SOP Team, Policy |
| Parameter at-1(a): all personnel |
| Parameter at-01\_odp.01: |
| Parameter at-01\_odp.02: |
| Parameter at-01\_odp.03: a Microsoft-wide |
| Parameter at-01\_odp.04: the Microsoft Information Risk Management Council (IRMC) organization |
| Parameter at-01\_odp.05: at least annually |
| Parameter at-01\_odp.06: significant changes |
| Parameter at-01\_odp.07: at least annually |
| Parameter at-01\_odp.08: significant changes |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☒ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AT-1 What is the solution and how is it implemented?** |
| **Part A1**  **Customer Responsibility**  The customer is responsible for developing, documenting, and disseminating awareness training policy and procedures that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.  **Azure**  Azure addresses the awareness and training policy as part of the Microsoft security policies, of which there are two sets: the Microsoft Security Policy (MSP) that is applicable to all Microsoft personnel, and the Microsoft Security Program Policy (MSPP), which is applicable to all Microsoft personnel that have a responsibility for security. The Microsoft Information Risk Management Council (IRMC) is the governance body with review and approval responsibility for the MSP and MSPP. Within Azure, the MSPP specifically applies to all Microsoft personnel with security objectives such as designing, building, and operating Azure and across all information and processes used in the conduct of Microsoft business. All Azure personnel are accountable and responsible for complying with these guiding principles within their designated roles. The policy addresses the following:  \* Security training  Additionally, the policy addresses the purpose, scope, roles, responsibilities, compliance requirements, and required coordination among the various Microsoft organizations that provide some level of support to all services. The policies indicate Microsoft management’s commitment and are a component of the risk management strategy which provides Azure personnel with a current set of clear and concise information security requirements.  The MSP is available to all Microsoft personnel on the Microsoft Policy website on the Microsoft intranet, and the MSPP and Security Standards are available through the Liquid tool, also on the Microsoft intranet. The Azure SOPs are stored in the Azure Security, Privacy & Compliance SharePoint site. This SharePoint site is accessible to all Azure personnel.  Service teams may supplement the Azure policies and procedures with offering-specific policies and procedures. Service-team-specific policies and procedures associated with awareness and training are documented and stored within internal Azure SharePoint sites. Only personnel with authorized credentials, adequate levels of permission, legitimate need to know, and specific roles and responsibilities are given access to the service-team-specific policies or procedures. |
| **Part A2**  **Customer Responsibility**  The customer is responsible for procedures to facilitate the implementation of the awareness and training policy and the associated awareness and training controls.  **Azure**  The Azure Security Security Education and Awareness Standard Operating Procedure (SOP) implements the awareness and training policy and associated controls and documents the following procedures:  \* Development of a program that requires all personnel to take the required training and any additional training based on individual job requirements  \* Educating personnel about specific procedures and topics related to their job function that support maintaining the confidentiality, integrity, and availability of Azure and its services  \* Standard approach, tools, and techniques used to implement and sustain the awareness program  Service teams may supplement the Azure policies and procedures with offering-specific policies and procedures. Service-team-specific policies and procedures associated with awareness and training are documented and stored within internal Azure SharePoint sites. Only personnel with authorized credentials, adequate levels of permission, legitimate need to know, and specific roles and responsibilities are given access to the service-team-specific policies or procedures. |
| **Part B**  **Customer Responsibility**  The customer is responsible for designating an official to manage the development, documentation, and dissemination of the awareness and training policy and procedures.  **Azure**  The Microsoft Information Risk Management Council (IRMC) organization is the governance body with approval responsibility for the Microsoft Security Policy (MSP) and Microsoft Security Program Policy (MSPP). The IRMC consists of representatives from security and risk management teams across Microsoft including Core Services Engineering and Operations (CSEO), Azure, and Global Security. The Customer Security Policy and Assurance (CSPA) organization manages the review and approval process and maintains the policies.  On an annual basis, the CST-SE conducts a line-by-line review of the MSP and MSPP. The Microsoft Security Policy (MSP) and Microsoft Security Program Policy (MSPP) Governance document describes each member’s role, types and frequency of review, escalation paths, approval process, and formal publishing procedures of the security policy. Throughout the year, if necessary, CST-SE may convene with the IRMC to conduct reviews after a significant review or change request. The approved policy update is published within the relevant tool on the Microsoft intranet. If service teams establish service-specific or team-specific policies, the respective service teams update the necessary policies at least annually. |
| **Part C1**  **Customer Responsibility**  The customer is responsible for reviewing and updating the current awareness and training policy on a regular basis and following organization-defined events.  **Azure**  The Azure team updates the Azure SOPs at least annually through a formal review process. If needed, the Azure team updates the SOP after a significant change affecting policy execution as well. If established, service-team-specific procedures are updated by their respective teams. The individual service teams review and update their respective SOPs at least annually and when required by a significant change. |
| **Part C2**  **Customer Responsibility**  The customer is responsible for reviewing and updating the current awareness and training procedures on a regular basis and following organization-defined events.  **Azure**  The Azure team updates the Azure SOPs at least annually through a formal review process. If needed, the Azure team updates the SOP after a significant change affecting policy execution as well. If established, service-team-specific procedures are updated by their respective teams. The individual service teams review and update their respective SOPs at least annually and when required by a significant change. |

## AT-2 Literacy Training and Awareness

a. Provide security and privacy literacy training to system users (including managers, senior executives, and contractors):

1. As part of initial training for new users and [at least annually] thereafter; and

2. When required by system changes or following [Assignment: organization-defined events];

b. Employ the following techniques to increase the security and privacy awareness of system users [techniques to be employed to increase the security and privacy awareness of system users are defined;];

c. Update literacy training and awareness content [at least annually] and following [events that would require literacy training and awareness content to be updated are defined;] ; and

d. Incorporate lessons learned from internal or external security incidents or breaches into literacy training and awareness techniques.

|  |
| --- |
| **AT-2 Control Summary Information** |
| Responsible Roles: Training |
| Parameter at-2(a)(1): at least annually |
| Parameter at-2(a)(2): organization-defined events |
| Parameter at-02\_odp.01: |
| Parameter at-02\_odp.02: |
| Parameter at-02\_odp.03: |
| Parameter at-02\_odp.04: |
| Parameter at-02\_odp.05: awareness techniques |
| Parameter at-02\_odp.06: at least annually |
| Parameter at-02\_odp.07: organization-defined events |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AT-2 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  The customer is responsible for providing basic security awareness training to all users of customer-deployed resources as part of initial training.  **Azure**  The annual Security Foundations Training includes basic level training on how to detect, report and implement best practices to safeguard Microsoft and its customers. This course also covers the security requirements and expectations for elevated privileges in production environments. Engineering personnel participate in ongoing role-based security training through the STRIKE program. STRIKE provides regular 200-400 level sessions, labs, online courses, and material to engage, educate, and empower engineers to securely design and operate services.  Azure requires all personnel to complete the following training as part of their onboarding process:  \* Security Foundations Training – Azure new hire personnel are required to take the Security Foundations Training within thirty (30) days of employment, and annually thereafter. STRIKE training, covering security topics for engineering roles is recommended as part of continued learning. |
| **Part B**  **Customer Responsibility**  The customer is responsible for providing updated basic security awareness training to all users when required by changes to customer-deployed resources.  **Azure**  STRIKE and Security Foundations Training trainings are updated on a regular basis to account for updates or changes that render previous training inaccurate. The trainings are sent to personnel supporting the operations of Azure cloud environments through automated learning system communications. Training completions are documented and retained for investigation purposes. |
| **Part C**  **Customer Responsibility**  The customer is responsible for providing ongoing, periodic basic security awareness training to all users.  **Azure**  The annual Security Foundations Training includes basic level training on how to detect, report and implement best practices to safeguard Microsoft and its customers. Engineering personnel are recommended to participate in ongoing role-based security training through the STRIKE program. STRIKE provides regular 200-400 level sessions, labs, online courses, and materials to engage, educate and empower engineers to securely design and operate services. |

### AT-2(2) - Insider Threat

Provide literacy training on recognizing and reporting potential indicators of insider threat.

|  |
| --- |
| **AT-2(2) Control Summary Information** |
| Responsible Roles: Training |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AT-2(2) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for providing training on insider threats.  **Azure**  The annual Security Foundations Training includes information on recognizing and reporting potential indicators of insider threat as well as instruction for reporting suspicious and anomalous behavior. All personnel with elevated access to Azure are required to complete the Security Foundations Training. |

### AT-2(3) - Social Engineering and Mining

Provide literacy training on recognizing and reporting potential and actual instances of social engineering and social mining.

|  |
| --- |
| **AT-2(3) Control Summary Information** |
| Responsible Roles: Training |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AT-2(3) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for providing literacy training and awareness for their own personnel.  **Azure**  The annual STRIKE or security foundations training include basic level training on how to detect and report social engineering and social mining attempts including methods such as dumpster diving, phishing, pretexting, shoulder surfing, baiting, quid pro quo, thread-jacking, social media exploitation, tailgating, and telephone impersonation. |

## AT-3 Role-based Training

a. Provide role-based security and privacy training to personnel with the following roles and responsibilities: [Assignment: organization-defined roles and responsibilities]:

1. Before authorizing access to the system, information, or performing assigned duties, and [at least annually] thereafter; and

2. When required by system changes;

b. Update role-based training content [at least annually] and following [events that require role-based training content to be updated are defined;] ; and

c. Incorporate lessons learned from internal or external security incidents or breaches into role-based training.

|  |
| --- |
| **AT-3 Control Summary Information** |
| Responsible Roles: Training |
| Parameter at-3(a): organization-defined roles and responsibilities |
| Parameter at-03\_odp.01: |
| Parameter at-03\_odp.02: |
| Parameter at-03\_odp.03: at least annually |
| Parameter at-03\_odp.04: at least annually |
| Parameter at-03\_odp.05: organization-defined events |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AT-3 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  The customer is responsible for providing role-based security training to users before authorizing access to customer-deployed resources or performing assigned duties. The customer is also responsible for providing role-based security training to all identified roles when required by changes to customer-deployed resources.  **Azure**  Microsoft C+AI training and awareness components are classified into one of two types: Role-Based and Required.  **Role-Based Training**  Role-Based training is provided to help facilitate the understanding of security processes and procedures for a particular role an individual is placed in and is directly related to the job responsibilities of the individual. Role-Based training is offered to full-time personnel through the STRIKE program for engineering disciplines providing 200-400 level security training and best practices.  **Required Training**  Required training is mandatory security and awareness education that the Information Risk Management Council (IRMC) has specifically identified and defined as appropriate for Azure personnel based upon their organization. Required annual training includes Security Foundations Training for employees. STRIKE training is provided for continual learning of those in engineering roles. Azure personnel are required to take the above trainings as required by information system changes. |
| **Part B**  **Customer Responsibility**  The customer is responsible for updating role-based training at a defined frequency for customer-deployed resources.  **Azure**  Azure updates role-based training content through STRIKE program on at least annual basis. |
| **Part C**  **Customer Responsibility**  The customer is responsible for providing ongoing, periodic role-based security training to all identified roles. The customer is also responsible for incorporating lessons learned from internal or external security incidents or breaches into role-based training for customer-deployed resources.  **Azure**  The above training is required to be taken by personnel on an annual basis. Azure confirms a user has taken the training through the Microsoft Learning Program. Microsoft management communicates this responsibility to all applicable managers who grant access to Azure data. The Microsoft Learning Program incorporates lessons learned from internal and external security incidents or breached into the role-based trainings executed through STRIKE program. |

## AT-4 Training Records

a. Document and monitor information security and privacy training activities, including security and privacy awareness training and specific role-based security and privacy training; and

b. Retain individual training records for [five (5) years or 5 years after completion of a specific training program].

|  |
| --- |
| **AT-4 Control Summary Information** |
| Responsible Roles: Training |
| Parameter at-4(b): at least five (5) years or five (5) years after completion of a specific training program |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AT-4 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  The customer is responsible for documenting and monitoring all system security and privacy training activities for customer-deployed resources.  **Azure**  Azure utilizes SuccessFactors Learning Management System (LMS) to document and monitor security and privacy training. The LMS provides reporting to effectively manage and track security training participation. Security training and privacy training records are documented, monitored, and retained for at least five (5) years. |
| **Part B**  **Customer Responsibility**  The customer is responsible for retaining individual training records for users of customer-deployed resources.  **Azure**  Azure retains records of all security training for at least five (5) years in the LMS. |

# Audit and Accountability (AU)

## AU-1 Policy and Procedures

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (OneOrMore): organization-level;mission/business process-level;system-level] audit and accountability policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the audit and accountability policy and the associated audit and accountability controls;

b. Designate an [an official to manage the audit and accountability policy and procedures is defined;] to manage the development, documentation, and dissemination of the audit and accountability policy and procedures; and

c. Review and update the current audit and accountability:

1. Policy [at least annually] and following [events that would require the current audit and accountability policy to be reviewed and updated are defined;] ; and

2. Procedures [at least annually] and following [significant changes].

|  |
| --- |
| **AU-1 Control Summary Information** |
| Responsible Roles: SOP Team, Logging and Monitoring |
| Parameter au-1(a): all personnel |
| Parameter au-01\_odp.01: |
| Parameter au-01\_odp.02: |
| Parameter au-01\_odp.03: a Microsoft-wide |
| Parameter au-01\_odp.04: the Microsoft Information Risk Management Council (IRMC) organization |
| Parameter au-01\_odp.05: at least annually |
| Parameter au-01\_odp.06: significant changes |
| Parameter au-01\_odp.07: at least annually |
| Parameter au-01\_odp.08: significant changes |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☒ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AU-1 What is the solution and how is it implemented?** |
| **Part A1**  **Customer Responsibility**  The customer is responsible for developing, documenting and disseminating audit and accountability policy and procedures that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.  **Azure**  Azure addresses the audit and accountability policy as part of the Microsoft security policies, of which there are two sets: the Microsoft Security Policy (MSP) that is applicable to all Microsoft personnel, and the Microsoft Security Program Policy (MSPP), which is applicable to all per that have a responsibility for security. The Microsoft Information Risk Management Council (IRMC) is the governance body with review and approval responsibility for the MSP and MSPP. Within Azure, the MSPP specifically applies to all Microsoft personnel with security objectives such as designing, building, and operating Azure and across all information and processes used in the conduct of Microsoft business. All Azure personnel are accountable and responsible for complying with these guiding principles within their designated roles. The policy addresses the following:  \* Security logging, monitoring, and reporting  Additionally, the policy addresses the purpose, scope, roles, responsibilities, compliance requirements, and required coordination among the various Microsoft organizations that provide some level of support to all services. The policies indicate Microsoft management’s commitment and are a component of the risk management strategy which provides Azure personnel with a current set of clear and concise information security requirements.  The Azure Logging and Monitoring Standard Operating Procedure (SOP) implements the audit and accountability policy and associated controls and documents the following procedures:  \* Security monitoring  \* Protection of log information  \* Log retention  \* Near-real time alerting  The MSP is available to all Microsoft personnel on the Microsoft Policy website on the Microsoft intranet, and the MSPP and Security Standards are available through the Liquid tool, also on the Microsoft intranet. The Azure SOPs are stored in the Azure Security, Privacy & Compliance SharePoint site. This SharePoint site is accessible to all Azure personnel.  Service teams may supplement the Azure policies and procedures with offering-specific policies and procedures. Service-team-specific policies and procedures associated with audit and accountability are documented and stored within internal Azure SharePoint sites. Only personnel with authorized credentials, adequate levels of permission, legitimate need to know, and specific roles and responsibilities are given access to the service-team-specific policies or procedures. |
| **Part A2**  **Customer Responsibility**  The customer is responsible for procedures to facilitate the implementation of the audit and accountability policy and the associated audit and accountability controls.  **Azure**  The Azure Logging and Monitoring SOP implements the audit and accountability policy and associated controls and documents the following procedures:  \* Security monitoring  \* Protection of log information  \* Log retention  \* Near-real time alerting  Service teams may supplement the Azure policies and procedures with offering-specific policies and procedures. Service-team-specific policies and procedures associated with audit and accountability are documented and stored within internal Azure SharePoint sites. Only personnel with authorized credentials, adequate levels of permission, legitimate need to know, and specific roles and responsibilities are given access to the service-team-specific policies or procedures. |
| **Part B**  **Customer Responsibility**  The customer is responsible for designating an official to manage the development, documentation, and dissemination of the audit and accountability policy and procedures.  **Azure**  The Microsoft Information Risk Management Council (IRMC) organization is the governance body with approval responsibility for the Microsoft Security Policy (MSP) and Microsoft Security Program Policy (MSPP). The IRMC consists of representatives from security and risk management teams across Microsoft including Core Services Engineering and Operations (CSEO), Azure, and Global Security. The Customer Security and Trust: Security Engineering (CST-SE) organization manages the review and approval process and maintains the policies.  On an annual basis, the CST-SE conducts a line-by-line review of the MSP and MSPP. The Microsoft Security Policy (MSP) and Microsoft Security Program Policy (MSPP) Governance document describes each member’s role, types and frequency of review, escalation paths, approval process, and formal publishing procedures of the security policy. Throughout the year, if necessary, CST-SE may convene with the IRMC to conduct reviews after a significant review or change request. The approved policy update is published within the relevant tool on the Microsoft intranet. If service teams establish service-specific or team-specific policies, the respective service teams update the necessary policies at least annually. |
| **Part C1**  **Customer Responsibility**  The customer is responsible for reviewing and updating the current audit and accountability policy on a regular basis and following organization defined events.  **Azure**  The Azure team updates the Azure SOPs at least annually through a formal review process. If needed, the Azure team updates the SOP after a significant change affecting policy execution as well. If established, service-team-specific procedures are updated by their respective teams. The individual service teams review and update their respective SOPs at least annually and when required by a significant change. |
| **Part C2**  **Customer Responsibility**  The customer is responsible for reviewing and updating the current audit and accountability procedures on a regular basis and following organization defined events.  **Azure**  The Azure team updates the Azure SOPs at least annually through a formal review process. If needed, the Azure team updates the SOP after a significant change affecting policy execution as well. If established, service-team-specific procedures are updated by their respective teams. The individual service teams review and update their respective SOPs at least annually and when required by a significant change. |

## AU-2 Event Logging

a. Identify the types of events that the system is capable of logging in support of the audit function: [successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes];

b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged;

c. Specify the following event types for logging within the system: [organization-defined subset of the auditable events defined in AU-2a to be audited continually for each identified event.];

d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and

e. Review and update the event types selected for logging [annually and whenever there is a change in the threat environment].

Requirement: Coordination between service provider and consumer shall be documented and accepted by the JAB/AO.

(e) Guidance: Annually or whenever changes in the threat environment are communicated to the service provider by the JAB/AO.

|  |
| --- |
| **AU-2 Control Summary Information** |
| Responsible Roles: Logging and Monitoring, Networking, SDL, Compute |
| Parameter au-2(c): all auditable events defined in AU-02(a) per occurrence |
| Parameter au-02\_odp.01: successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For web applications: all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes |
| Parameter au-02\_odp.02: |
| Parameter au-02\_odp.03: |
| Parameter au-02\_odp.04: at least annually |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AU-2 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for identifying the types of events that the customer-deployed resources are capable of logging.  **Azure**  The Azure Security Logging and Monitoring (SLAM) team and the Security Response Team have developed sets of auditable events for Azure assets based on ongoing risk assessments of the system which incorporate government and industry baselines and requirements, identified vulnerabilities, business requirements, and Azure and C+AI Security Standards. The event sets are reviewed by the SLAM and Security Response Team when a significant change to the system is made to ensure any vulnerabilities exposed are being addressed by the set of auditable events. New events are incorporated when a new asset class is brought online or when a vulnerability or threat is identified through security assessments, security bulletins, and more.  Azure Security Pack (AzSecPack) and Geneva Monitoring, composed of Logs, Metrics, and Analytics, are the main drivers of audit log collection. AzSecPack is deployed via the Geneva Monitoring Agent (MA), covering both Windows and Linux operating systems and operating as the raw event source. AzSecPack monitors events throughout the Azure environment in an automated fashion, feeding logs through Azure Security Monitoring (ASM), Kusto, and SCUBA to identify and alert on events of interest. Personnel can use Kusto and Jarvis to examine the logs in human-readable format.  All asset types supporting Azure’s cloud environments are configured to log the following events:  Successful and unsuccessful account logon events, successful and unsuccessful attempts to access, modify, or delete privileges, account management events, privileged activities, security objects, security levels, or categories of information (e.g., classification levels), object access, policy change, privilege functions, process tracking, starting and ending time for user access to the system, concurrent logons from different workstations, successful and unsuccessful accesses to objects, all program initiations, all direct access to the information system, all account creations, modifications, disabling, and terminations, all kernel module load, unload, all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes and restart, and system events.  **Servers**  For server assets, the audit policy is set as part of installing AzSecPack on a given server, required for Azure. AzSecPack collects all server asset logs and sends them to the Geneva Monitoring Agent (MA), a client executable that is run on the asset to collect logs and upload them to Azure storage accounts owned by the service team. Geneva Monitoring then ingests and analyzes the logs via multiple detection services, including but not limited to Azure Security Monitoring (ASM), Kusto, and SCUBA, for events requiring alerting.  **Network Devices**  Utilizing the audit log collection tool protocol and event collection infrastructure, Azure retrieves events from network device syslog. The logs are sent to servers running AzSecPack for storage and processing for format and content via Geneva Monitoring. Geneva Monitoring then ingests and analyzes the logs via multiple detection services, including but not limited to Azure Security Monitoring (ASM), Kusto, and SCUBA, for events requiring alerting.  **Azure Services**  Service teams configure their service to generate audit logs based upon the service-specific risk assessment. Service teams are responsible for configuring service-layer audit logs as a part of the Security Development Lifecycle (SDL) process using the OpenTelemetry Audit instrumentation, feeding into the Geneva MA and the pipeline described above. |
| **Part B**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for coordinating with other entities within its organization to guide the selection of auditable events for customer-deployed resources.  **Azure**  Azure incorporates business requirements from Azure as a whole and from individual service teams when developing the set of auditable events. The Azure Security team meets on a formal and regular basis to coordinate and collaborate on security, auditing, and monitoring objectives. |
| **Part C**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for selecting a subset of the events defined in AU-02.a to be audited on customer-deployed resources.  **Azure**  **Servers**  The configuration file for AzSecPack specifies the audit events. Events are audited continually in near-real time. These events are based on the assessment of risk to the system and the Microsoft Security Standards used across the organization. These events align with the server baselines updated semi-annually and available to all Microsoft users.  **Network Devices**  While each network device type has specific events and metadata options, Azure Networking selects the level of auditing to meet or exceed the audited events defined by the Azure SLAM team and configures the devices appropriately. |
| **Part D**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for ensuring the list of auditable events supports after-the-fact investigations of customer-deployed resources.  **Azure**  Designated Azure personnel select which auditable events are to be audited, and Azure assets generate such audit records which enable Azure Security to support after-the-fact investigations of security incidents. The Security Response Team is involved in determining which events should be audited to support the incident management process and it has been determined that the selected events are sufficient to support the after-the-fact investigations of security incidents. Azure performs a review of the events to be audited within Azure at least annually, using several sources of input including security architects, incident management personnel, security analysts, and system operators, to determine that the list of auditable events is adequate to support after-the-fact investigations of security incidents. |
| **Part E**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for reviewing and updating the event types selected for logging on customer-deployed resources at least annually.  **Azure**  Azure Security reviews the events to be audited within Azure at least annually using several sources of input, including the Security Engineering Team, Service Engineer Operations, Azure Engineers, Azure security architects, incident management personnel, Azure security analysts, and system operators to determine whether the list of auditable events is adequate to support after-the-fact investigations of security incidents. C+AI Security also reviews the events to be audited whenever changes in the threat environment are identified internally or communicated to Azure by the FedRAMP JAB, DISA/DoD authorizing officials, and other regulators as required. If updates are needed, C+AI Security updates the list upon completion of the review.  In addition to the annual and threat-based reviews, C+AI Security performs ongoing reviews of rule sets when Security Response Team Tier 2 personnel process events. If the rule sets are deemed insufficient because of an event review, after being vetted by the Security Response Team leader, feature requests are placed into the bug tracking tool to change rules to the auditable events. These changes are subject to peer review. |

## AU-3 Content of Audit Records

Ensure that audit records contain information that establishes the following:

a. What type of event occurred;

b. When the event occurred;

c. Where the event occurred;

d. Source of the event;

e. Outcome of the event; and

f. Identity of any individuals, subjects, or objects/entities associated with the event.

|  |
| --- |
| **AU-3 Control Summary Information** |
| Responsible Roles: Logging and Monitoring, Networking, Compute |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AU-3 What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for configuring Azure auditing capabilities on customer-deployed resources to generate audit records containing the following: what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any subjects associated with the event.  **Azure**  Azure utilizes auditing configurations enforced by AzSecPack and the Security Development Lifecycle (SDL) process that ensure the auditable event metadata contains at a minimum what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identifiers associated with the event. Exactly how this is captured varies for each asset, but the Azure configuration baselines for servers, network devices, and services include the minimum requirements specified above. |

### AU-3(1) - Additional Audit Information

Generate audit records containing the following additional information: [session, connection, transaction, or activity duration; for client-server transactions, the number of bytes received and bytes sent; additional informational messages to diagnose or identify the event; characteristics that describe or identify the object or resource being acted upon; individual identities of group account users; full-text of privileged commands].

Guidance: For client-server transactions, the number of bytes sent and received gives bidirectional transfer information that can be helpful during an investigation or inquiry.

|  |
| --- |
| **AU-3(1) Control Summary Information** |
| Responsible Roles: Logging and Monitoring, Networking, Compute |
| Parameter au-03.01\_odp: session, connection, transaction, or activity duration; for client-server transactions, the number of bytes received, and bytes sent; additional informational messages to diagnose or identify the event; characteristics that describe or identify the object or resource being acted upon; ; individual identities of group account users; full-text of privileged commands (FedRAMP-Defined for au-3.1) |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AU-3(1) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for configuring Azure auditing capabilities on customer-deployed resources to ensure organizational audit record content requirements are implemented.  **Azure**  Azure collects audit record content including the additional content required. This content includes informational messages to diagnose or identify events, characteristics that describe or identify the object or resource being acted upon, and the number of bytes received, and bytes sent, all of which vary by event type and asset. The session, connection, transaction, or activity duration can be obtained by analyzing the audit records collected; events related to sessions, connections and transactions contain timestamps which can be analyzed to determine duration. |

## AU-4 Audit Log Storage Capacity

Allocate audit log storage capacity to accommodate [audit log retention requirements are defined;].

|  |
| --- |
| **AU-4 Control Summary Information** |
| Responsible Roles: Logging and Monitoring, Networking |
| Parameter au-4: the ability to retain at least ninety (90) days’ worth of logs online and one (1) year offline |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AU-4 What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for allocating audit log storage capacity for customer-deployed resources. Additionally, the customer should consider the retention period defined in AU-11 when allocating storage capacity for audit records.  **Azure**  Audit records for each Azure service are captured by the Geneva Monitoring Agent (MA) and retained in a service-specific Azure storage account. The MA collects data from the service assets and automatically uploads to the service storage account. Each storage account is allocated sufficient storage capacity for the retention of at least ninety (90) days’ worth of logs online and is monitored for usage by the service teams. If a storage account is near capacity, either - service teams are notified by Azure Storage automatically and the service teams creates an additional storage account or expand the current account’s capacity; or, if the service team has configured Azure Storage for auto-expansion, the storage is increased as needed. Each service team is responsible for its own log capacity planning. If the service team does not expand capacity for any reason, due to the high volume of events received, Azure audit collection settings are to overwrite when capacity is exceeded.  The MA then sends the collected logs from the service-specific storage into a central log storage cluster known as the parsing engine. This local cluster stores centrally aggregated log data for the purposes of standardizing the ingested log data, such as time, date, field titles, etc., and parsing the data for alerting via multiple microservices. The logs do not reside on these servers long-term; once parsed, logs are provided to Kusto and Jarvis. Kusto and Jarvis then retain the parsed data as read-only, ensuring the integrity of the centralized logs, automatically growing the backend data storage. There is no hard limit associated with the central storage.  Azure currently defines baseline requirements for local security audit log storage capacity to a window of at least ten (10) minutes of events on even Azure’s most active hosts. Events are continuously sent to Geneva Monitoring, which has adequate storage capacity to handle the volume of events captured due to auto-expansion. In the event of an audit failure or audit storage capacity being reached, Azure monitoring tools generate near-real time alerts to the C+AI Security Engineering team, who are assigned to address the processing failure. |

## AU-5 Response to Audit Logging Process Failures

a. Alert [personnel or roles receiving audit logging process failure alerts are defined;] within [time period for personnel or roles receiving audit logging process failure alerts is defined;] in the event of an audit logging process failure; and

b. Take the following additional actions: [overwrite oldest record].

|  |
| --- |
| **AU-5 Control Summary Information** |
| Responsible Roles: Logging and Monitoring |
| Parameter au-05\_odp.01: Service Engineer Operations personnel; Azure Security if failure is confirmed |
| Parameter au-05\_odp.02: immediate notification and investigation |
| Parameter au-05\_odp.03: overwrite oldest audit records if necessary; shut down if necessary |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AU-5 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for providing alerts in response to audit processing failures (e.g., storage quota is reached, audit hardware/software errors) of customer-deployed resources.  **Azure**  The Geneva Monitoring Agent (MA) is responsible for capturing log events and storing them in storage accounts specific to each service team. Incident Management (IcM) is an automated mechanism for scanning log storage and raising alerts when specific predefined criteria is met. IcM generates email notifications and creates a corresponding IcM ticket for action. IcM actively monitors Azure based on the filters and the thresholds identified within the rules defined by the Azure Security team and respective service teams. Key alerts include, but are not limited to, if AzSecPack is not installed, if audit data is not being received, and if the data decreases by a specific percentage, indicating an audit logging failure somewhere in the log pipeline. All alerts follow the incident management procedures, which include analysis to determine whether further action is necessary by either the service team or Security Response Team. |
| **Part B**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for taking action when audit processing failures occur for customer-deployed resources.  **Azure**  In the event of an audit failure or audit storage capacity being reached, monitoring tools alert the C+AI Security Engineering team in near real time, who are assigned to address the processing failure. Alerts for audit processing failures are investigated immediately following the incident management process and appropriate actions are taken in accordance with the incident management process. In addition, if the failure is that the storage repository is full, Azure is configured to overwrite the oldest data to preserve the most recent information for after-the-fact investigations. |

### AU-5(1) - Storage Capacity Warning

Provide a warning to [personnel, roles, and/or locations to be warned when allocated audit log storage volume reaches a percentage of repository maximum audit log storage capacity.] within [time period for defined personnel, roles, and/or locations to be warned when allocated audit log storage volume reaches a percentage of repository maximum audit log storage capacity is defined;] when allocated audit log storage volume reaches [75%, or one month before expected negative impact] of repository maximum audit log storage capacity.

|  |
| --- |
| **AU-5(1) Control Summary Information** |
| Responsible Roles: Logging and Monitoring, Storage |
| Parameter au-05.01\_odp.01: C+AI Security Engineering team |
| Parameter au-05.01\_odp.02: twenty-four (24) hours; in real time |
| Parameter au-05.01\_odp.03: a service-team-defined percentage; a point of failure |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AU-5(1) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for configuring an audit record storage capacity warning for customer-deployed resources including the percentage of storage capacity at which a warning is required; the time period within which the warning must occur; and the personnel, roles, and/or locations to be notified.  **Azure**  Most services use Azure Storage auto-expansion for service team storage of logs. When the storage account reaches a specific threshold of 90%, Azure Storage automatically provisions additional space. For services who have not transitioned to auto-expansion, automated messages are sent out in near-real time, alerting service teams whenever a pre-determined threshold of 80% and 95% of storage capacity is crossed. If the storage repository is full because a service team was unable to resolve the alert in time, Azure is configured to overwrite the oldest data to preserve the most recent information for after-the-fact investigations. |

### AU-5(2) - Real-time Alerts

Provide an alert within [real-time] to [service provider personnel with authority to address failed audit events] when the following audit failure events occur: [audit failure events requiring real-time alerts, as defined by organization audit policy].

|  |
| --- |
| **AU-5(2) Control Summary Information** |
| Responsible Roles: Logging and Monitoring |
| Parameter au-05.02\_odp.01: near-real time |
| Parameter au-05.02\_odp.02: appropriate service team personnel, security engineering teams |
| Parameter au-05.02\_odp.03: events defined by each service team such as hardware or software failures, nearing storage capacity |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AU-5(2) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for providing real-time alerts for audit event failures for customer-deployed resources.  **Azure**  The Geneva Monitoring Agent (MA) is responsible for capturing log events and storing them in storage accounts specific to each service team. Incident Management (IcM) is an automated mechanism for scanning log storage and raising alerts in real-time period when specific predefined criteria is met. IcM generates email notifications and creates a corresponding IcM ticket for action in real-time period. IcM actively monitors Azure based on the filters and the thresholds identified within the rules defined by the Azure Security team and respective service teams. Key alerts include, but are not limited to, if AzSecPack is not installed, if audit data is not being received, and if the data decreases by a specific percentage, indicating an audit logging failure somewhere in the log pipeline. All alerts follow the incident management procedures, which include analysis to determine whether further action is necessary by either the service team or Security Response Team. |

## AU-6 Audit Record Review, Analysis, and Reporting

a. Review and analyze system audit records [at least weekly] for indications of [inappropriate or unusual activity is defined;] and the potential impact of the inappropriate or unusual activity;

b. Report findings to [personnel or roles to receive findings from reviews and analyses of system records is/are defined;] ; and

c. Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.

Requirement: Coordination between service provider and consumer shall be documented and accepted by the JAB/AO. In multi-tenant environments, capability and means for providing review, analysis, and reporting to consumer for data pertaining to consumer shall be documented.

|  |
| --- |
| **AU-6 Control Summary Information** |
| Responsible Roles: Logging and Monitoring, Incident Response |
| Parameter au-06\_odp.01: in real time |
| Parameter au-06\_odp.02: indications of compromise identified in SI-04(05) or events that meet a pattern of a known attack methodology |
| Parameter au-06\_odp.03: Azure LiveSite team, ISSO, and ISSM as applicable |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AU-6 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  The customer is responsible for reviewing and analyzing audit records of customer-deployed resources to identify inappropriate or unusual activity and the potential impact.  **Azure**  Due to the size and complexity of the Azure environment, Azure utilizes log event forwarding tools to record events across all Azure assets and utilizes monitoring tools to automatically correlate and analyze the events gathered by each logging tool. Log reviews cannot be conducted manually in the Azure environment due to the high volume of events. Instead, Azure implements automated methods to perform review, analysis, and reporting of logs.  Azure implements tooling such as Azure Security Monitoring (ASM) and SCUBA to directly alert the appropriate personnel of security-relevant events in a variety of ways, including Service 360 (S360) notifications, Incident Management (IcM) tickets, and work items. These tools utilize audit policies and detections that report events to the Microsoft Operations Center (MOC), Security Response Team, and service teams as appropriate. The policies are tuned to alert on events of immediate concern.  There are multiple detection authoring teams across Azure. This includes data scientists working on Microsoft Defender for Cloud and the Microsoft Threat Intelligence Center (MSTIC) who write detections for both external customer use via ASC and enable coverage of applicable detections for internal Azure services via the logging and monitoring pipeline. Examples of the detections are documented in the help topic for ASC detection capabilities at the link below.  <https://docs.microsoft.com/en-us/azure/security-center/security-center-detection-capabilities>  This includes integrated threat intelligence which looks for known bad actors by leveraging global threat intelligence from Microsoft products and services, the Microsoft Digital Crimes Unit (DCU), the Microsoft Security Response Center (MSRC), and external feeds, behavioral analytics, which applies known patterns to discover malicious behavior, and anomaly detection, which uses statistical profiling to build a historical baseline and alerts on deviations from established baselines that conform to a potential attack vector.  Example of detections running for internal Azure services include suspicious process execution, malicious PowerShell scripts, lateral movement and internal reconnaissance, and hidden virus, malware, and exploitation attempts. These detections are routed to MSRC for triage and investigation. The ASM team has atomic near-real-time monitors for unexpected asset access, virus and malware, and audit processing failures such as clearing the security event log and system time changes. The alerts are auto routed to services for review, except for identified high value assets (HVA) where the alerts are centrally triaged by the Security Response Team.  Once the raw logs are automatically correlated and processed, the appropriate teams review and analyze alerts generated by the detections and automated review of audit records in real time, customer request or escalation, or any other functionality impacting the alert in production. Groups of these correlated events that meet a pattern of a known attack methodology are collected and delivered to appropriate personnel via IcM, email, or work item. Personnel correlate alerts and append them to tickets for review and analysis, and if necessary for future authoring and refinement of new or existing detections. The alerting system provides a response capability twenty-four (24) hours a day, seven (7) days a week. Troubleshooting Guides (TSGs) applied to work tickets provide instructions for the escalation of certain events to response personnel. |
| **Part B**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for reporting findings of inappropriate or unusual activity (defined in AU-06.a) on customer-deployed resources.  **Azure**  Azure configures the detections and resulting alerts to be sent to the appropriate parties for resolution. Depending on the alert, this can include the service team or the Security Response Team. For example, use of Break-Glass account generates an alert to the service team owning the subscription in which Break-Glass account access was utilized. Alternatively, malicious PowerShell scripts are routed to the Security Response Team. Regardless of which team the alert is routed to, all service teams, Azure personnel, and external customers can escalate an incident or report a new one. |
| **Part C**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for adjusting the level of audit review, analysis, and reporting for customer-deployed resources when there is a change in risk based on information provided by law enforcement, intelligence, or other credible sources.  **Azure**  Azure Security receives alerts from vendor websites, other third-party services such as Internet Security Systems, US-CERT advisories and alerts, and Microsoft-published bulletins and adjusts the level of auditing in two ways - first, Azure notifies Azure service teams if a change in the level of monitoring is necessary due to indications of increased risk, and service teams adjust monitoring accordingly. Second, Azure tailors detections to look for specific threats based on the nature of the risk to Azure operations and assets.  When circumstances dictate a review of the auditing procedures, such as a change in risk level based on law enforcement information, intelligence information, or other credible sources of information as provided, the C+AI Security team may make the decision to modify the audit procedures, including stakeholders from the Security Response Team, Security Governance Platform, Compliance, Risk, Architecture, Threat, and Strategy, Security Architecture, and Security Engineering. C+AI Security may also make updates whenever a change occurs in the threat environment as defined by authoritative sources. |

### AU-6(1) - Automated Process Integration

Integrate audit record review, analysis, and reporting processes using [automated mechanisms used for integrating audit record review, analysis, and reporting processes are defined;].

|  |
| --- |
| **AU-6(1) Control Summary Information** |
| Responsible Roles: Logging and Monitoring, Incident Response |
| Parameter au-06.01\_odp: automated mechanisms |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AU-6(1) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for automating the audit review, analysis, and reporting of suspicious activities within customer-deployed resources.  **Azure**  Audit review, analysis, and reporting processes are automated using Geneva Monitoring, Azure Security Monitoring (ASM), SCUBA, and other tools. ASM and SCUBA analyze event distribution to identify spikes in event traffic and aggregate analysis such as anomaly detection, filtering and allowlisting rules, specific event alert triggers, and more. ASM can generate summary reports using predefined queries. Geneva Monitoring applies correlation logic and intelligence to the audit log events. All detection services can generate alerts automatically. |

### AU-6(3) - Correlate Audit Record Repositories

Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.

|  |
| --- |
| **AU-6(3) Control Summary Information** |
| Responsible Roles: Logging and Monitoring, Incident Response |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AU-6(3) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for analyzing and correlating audit records (defined in AU-06) across customer-deployed repositories.  **Azure**  Due to the size and complexity of the Azure environment, Azure utilizes log event forwarding tools to record events across all Azure assets and utilizes monitoring tools to automatically correlate and analyze the events gathered by each logging tool. Log reviews cannot be conducted manually in the Azure environment due to the high volume of events. Instead, Azure implements automated methods to perform review, analysis, and reporting of logs.  Azure implements tooling such as Azure Security Monitoring (ASM) and SCUBA to directly alert the appropriate personnel of security-relevant events in a variety of ways, including Service 360 (S360) notifications, Incident Management (IcM) tickets, and work items. These tools utilize audit policies and detections that report events to the Microsoft Operations Center (MOC), Security Response Team, and service teams as appropriate. The policies are tuned to alert on events of immediate concern. |

### AU-6(4) - Central Review and Analysis

Provide and implement the capability to centrally review and analyze audit records from multiple components within the system.

|  |
| --- |
| **AU-6(4) Control Summary Information** |
| Responsible Roles: Logging and Monitoring, Incident Response |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AU-6(4) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for providing and implementing the capability to centrally review and analyze audit records collected from multiple components within the system.  **Azure**  Due to the size and complexity of the Azure environment, Azure utilizes log event forwarding tools to record events across all Azure assets and utilizes monitoring tools to automatically correlate and analyze the events gathered by each logging tool. Log reviews cannot be conducted manually in the Azure environment due to the high volume of events. Instead, Azure implements automated methods to perform review, analysis, and reporting of logs.  Azure implements tooling such as Azure Security Monitoring (ASM) and SCUBA to directly alert the appropriate personnel of security-relevant events in a variety of ways, including Service 360 (S360) notifications, Incident Management (IcM) tickets, and work items. These tools utilize audit policies and detections that report events to the Microsoft Operations Center (MOC), Security Response Team, and service teams as appropriate. The policies are tuned to alert on events of immediate concern. |

### AU-6(5) - Integrated Analysis of Audit Records

Integrate analysis of audit records with analysis of [Selection (OneOrMore): vulnerability scanning information;performance data;system monitoring information;[data/information collected from other sources to be analyzed is defined (if selected);] ] to further enhance the ability to identify inappropriate or unusual activity.

|  |
| --- |
| **AU-6(5) Control Summary Information** |
| Responsible Roles: Logging and Monitoring, Incident Response |
| Parameter au-06.05\_odp.01: vulnerability scanning information, performance data, information system monitoring information, penetration test data |
| Parameter au-06.05\_odp.02: |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AU-6(5) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for integrating audit record analysis with analysis of data/information collected from other sources to further identify suspicious activity within customer-deployed resources.  **Azure**  Azure correlates vulnerability scanning information with internal and external penetration test results and audit records to gain a more complete picture of potential exploits and to enhance the ability to detect inappropriate activity, should it occur. Additionally, Azure uses vulnerability scanning reports in conjunction with performance and system monitoring data to identify unusual activity. Azure combines the use of various sources of intelligence to aid incident investigation on an as-needed basis, including the use of audit logging data, incident response reports, vulnerability scan data, and penetration testing results. The correlation of this information is part of the identification phase of the incident management process and aids in discovering the presence of inappropriate activity in the Azure environment. |

### AU-6(6) - Correlation with Physical Monitoring

Correlate information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity.

Requirement: Coordination between service provider and consumer shall be documented and accepted by the JAB/AO.

|  |
| --- |
| **AU-6(6) Control Summary Information** |
| Responsible Roles: Incident Response |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AU-6(6) What is the solution and how is it implemented?** |
| **Azure**  The Azure Security Response Team combine the analysis of audit records with physical security monitoring data as needed to aid in incident investigations. Any breaches or physical security incidents are reported through the incident reporting process by the physical security team if the physical security incident could potentially impact logical security. The Security Response Team then compares information from such physical security incidents to audit logging records to further identify and investigate suspicious behavior. Furthermore, when a physical incident is reported, the Security Response Team uses the related physical monitoring data and correlates it with audit records to determine if there was any associated logical breach or suspicious behavior in the Azure environment. |

### AU-6(7) - Permitted Actions

Specify the permitted actions for each [Selection (OneOrMore): system process;role;user] associated with the review, analysis, and reporting of audit record information.

|  |
| --- |
| **AU-6(7) Control Summary Information** |
| Responsible Roles: Incident Response |
| Parameter au-06.07\_odp: information system process, role, or user |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AU-6(7) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for specifying the permitted actions associated with the review, analysis, and reporting of customer-controlled audit information.  **Azure**  Azure specifies the permitted actions for each process, role, or user via role-based access control. Security groups are defined in OneIdentityand MyAccess; each security group has specified access rights and permitted actions. Users are added to security groups via the account management process managed and implemented by Azure service teams.  The Azure Security Response Team, responsible for both incident management and monitoring, define the roles and responsibilities in the Azure Incident Management Standard Operating Procedure (SOP). Additionally, the Security Response Team performs both incident management and monitors analytics from the logging services. Only authorized members of the Security Response Team have access to audit log information. This information is only used to aid in incident management and investigation and is not available to personnel outside the incident management function. |

## AU-7 Audit Record Reduction and Report Generation

Provide and implement an audit record reduction and report generation capability that:

a. Supports on-demand audit record review, analysis, and reporting requirements and after-the-fact investigations of incidents; and

b. Does not alter the original content or time ordering of audit records.

|  |
| --- |
| **AU-7 Control Summary Information** |
| Responsible Roles: Logging and Monitoring |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AU-7 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for providing and implementing an audit reduction and report generation capability for customer-deployed resources, including the support of on-demand audit review, analysis, and reporting requirements, and after-the-fact investigations of security incidents.  **Azure**  Azure service teams leverage Geneva Monitoring and SCUBA as part of environment-wide monitoring solutions. Geneva Monitoring and SCUBA digest large amounts of log data into human-readable alerting and reports. All events are logged and available for human review as needed, but all events are reviewed automatically and known good activity is filtered out from alerting on an ongoing basis. Events that meet detection criteria, such as those that could indicate attacks or misuse, are automatically flagged and escalated as alerts in S360 or work items in IcM or DevOps. These are sent directly to Azure service teams for clarification and feedback or escalated within the Security Response Team for incident management. |
| **Part B**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for ensuring the original content and time ordering of customer-controlled audit records are not altered.  **Azure**  The tools used in Azure to collect and process audit records do not permanently or irreversibly alter the original audit record content or time ordering. Kusto and Jarvis by default are not an updateable data storage system, processing logs as read-only. They do not provide any update or delete functionality. |

### AU-7(1) - Automatic Processing

Provide and implement the capability to process, sort, and search audit records for events of interest based on the following content: [fields within audit records that can be processed, sorted, or searched are defined;].

|  |
| --- |
| **AU-7(1) Control Summary Information** |
| Responsible Roles: Logging and Monitoring |
| Parameter au-07.01\_odp: all fields within audit records |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AU-7(1) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for providing the capability to process, sort and search audit records for events of interest based on organization-defined audit fields within audit records.  **Azure**  The incoming stream of events are aggregated, correlated, duplicated, and reduced into security- or service-relevant alerts and alarms that are used by the service teams and Security Response Team to analyze and respond appropriately to suspicious activity. Authorized personnel can query Geneva Monitoring and Jarvis, the Azure security incident and event management tools, to sort and search audit records for events of interest based on the content of all captured fields and generate reports that are used to review events or investigate specific activities. |

## AU-8 Time Stamps

a. Use internal system clocks to generate time stamps for audit records; and

b. Record time stamps for audit records that meet [one second granularity of time measurement] and that use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp.

|  |
| --- |
| **AU-8 Control Summary Information** |
| Responsible Roles: Logging and Monitoring, Networking, Compute |
| Parameter au-8(b): under one second granularity of time measurement |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AU-8 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  The customer is responsible for generating time stamps for audit records of customer-deployed resources using the internal system clock.  **Azure**  For all Azure assets, audit records generated capture the time stamp from the internal system clock of the asset that generated the event. Azure implements time stamps stored in UTC format using NTP Version 3, which is based on the time standard from the United States Naval Observatory. NTP is a protocol designed to synchronize the clocks of computers over a network to a common time base.  Azure uses stratum 1 time sources in the United States for the infrastructure. Every pair of redundant core Azure datacenter routers (DCRs) provides clock information to the Azure datacenter devices. The overall approach is to use the DCRs as NTP servers. The DCRs synchronize off the authoritative stratum 1 time sources, with Azure equipment synchronizing off the DCRs.  The Azure NTP stratum 1 time servers sync off of the Global Positioning System (GPS) satellites. The same IP addresses for NTP are configured on the DCRs in each Azure datacenter, with routing tables being used to determine the closest source to any given client via an anycast-style solution. These IP addresses are in management IP space and synchronization is done over the management network, which addresses ACL issues. |
| **Part B**  **Customer Responsibility**  The customer is responsible for ensuring customer-controlled audit records have time stamps that are recorded and can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT).  **Azure**  Azure records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC). Time stamps are generated either in UTC directly or in local time with an offset from UTC. Azure time stamps are precise at least to the millisecond. |

## AU-9 Protection of Audit Information

a. Protect audit information and audit logging tools from unauthorized access, modification, and deletion; and

b. Alert [personnel or roles to be alerted upon detection of unauthorized access, modification, or deletion of audit information is/are defined;] upon detection of unauthorized access, modification, or deletion of audit information.

|  |
| --- |
| **AU-9 Control Summary Information** |
| Responsible Roles: Logging and Monitoring |
| Parameter au-9(b): Azure LiveSite team, ISSO, and ISSM as applicable |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AU-9 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for preventing unauthorized access to audit information and audit logging tools.  **Azure**  Only service team personnel for the specific asset within Azure have access to security logs on the local asset via the role-based access control (RBAC) implemented via OneIdentity. Azure implements protection of audit information using an authenticated and encrypted connection from the local asset of log generation to the centralized audit collection services using the Geneva Monitoring Agent (MA). Access to the centralized audit collection services and storage is restricted to the Security Engineering and Operations groups based on the standard access groups defined for Azure.  Only authorized service team personnel are allowed access to the actual audit records, and their assigned rights prohibit them from modifying or deleting audit information. Even if a user is able to clear local asset log data after elevating permissions via an approved JIT request, the action of cleaning the data is logged, and the cleared log data is present on Geneva Monitoring storage due to central ingestion.  The following mechanisms are used to protect log information in transit and at rest:  \* Logs on the local asset can only be accessed through direct login to the asset.  \* The transfer of logs from the local asset to the service team and central storage accounts occurs over an HTTPS connection.  \* Read-only access to logs in Geneva Monitoring storage for Azure users is enabled through the Geneva Monitoring front-end portal. The access is restricted through AD security groups which are managed through OneIdentity. |
| **Part B**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible alerting organization-defined personnel or roles upon detection of unauthorized access, modification, or deletion of audit information.  **Azure**  Azure configures the detections and resulting alerts to be sent to the appropriate parties for resolution. Depending on the alert, this can include the service team or the Security Response Team. For example, use of Break-Glass account generates an alert to the service team owning the subscription in which Break-Glass account access was utilized. Alternatively, malicious PowerShell scripts are routed to the Security Response Team. Regardless of which team the alert is routed to, all service teams, Azure personnel, and external customers can escalate an incident or report a new one. |

### AU-9(2) - Store on Separate Physical Systems or Components

Store audit records [at least weekly] in a repository that is part of a physically different system or system component than the system or component being audited.

|  |
| --- |
| **AU-9(2) Control Summary Information** |
| Responsible Roles: Logging and Monitoring |
| Parameter au-09.02\_odp: continually and daily |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AU-9(2) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for backing up customer-controlled audit records in a repository that is part of a physically different system at the required frequency.  **Azure**  Audit backs up logs to the service team Azure Storage accounts in near-real time. If this near-real-time log shipping fails, logs are retained on the local asset until they can be exported to the appropriate central storage location. |

### AU-9(3) - Cryptographic Protection

Implement cryptographic mechanisms to protect the integrity of audit information and audit tools.

Guidance: Note that this enhancement requires the use of cryptography which must be compliant with Federal requirements and utilize FIPS validated or NSA approved cryptography (see SC-13.)

|  |
| --- |
| **AU-9(3) Control Summary Information** |
| Responsible Roles: Logging and Monitoring, SDL, Storage |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AU-9(3) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for maintaining the integrity of the customer-controlled audit system.  **Azure**  Azure cryptographically protects all audit log data stored within the Azure Storage accounts used for audit log retention as a native feature of Azure Storage. In addition, Kusto and Jarvis storage is read-only by design, and once logs are ingested and stored, cannot be altered or deleted in any way.  Audit tooling is protected in the same method as all other Azure code, via the code signing process as part of the Security Development Lifecycle (SDL) implementation and Azure System Lockdown (AzSysLock) validation, currently operating in Audit Mode. AzSysLock alerts the affected Azure service team when unsigned code is installed and run within Azure. When Enforcement Mode is activated, AzSysLock will block unsigned code. In the scenario of AzSysLock feature is turned off for Azure services, detections are sent to Azure service and security teams for activation actions. |

### AU-9(4) - Access by Subset of Privileged Users

Authorize access to management of audit logging functionality to only [a subset of privileged users or roles authorized to access management of audit logging functionality is defined;].

|  |
| --- |
| **AU-9(4) Control Summary Information** |
| Responsible Roles: Logging and Monitoring |
| Parameter au-09.04\_odp: Service Engineer Operations |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AU-9(4) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for restricting the management of customer-controlled audit resources to authorized users.  **Azure**  Azure restricts management of audit functionality within Azure to the service teams and Azure Security team with approved least privilege and separation of duties role-based access. If the audit logs contain customer information, the logs are further restricted to a defined access group managed by the service team and restricted to need-to-know personnel. These personnel do not have the ability to modify or delete audit records from the central log repositories, and if they disable logging, that action itself is logged and investigated. |

## AU-10 Non-repudiation

Provide irrefutable evidence that an individual (or process acting on behalf of an individual) has performed [minimum actions including the addition, modification, deletion, approval, sending, or receiving of data].

|  |
| --- |
| **AU-10 Control Summary Information** |
| Responsible Roles: Logging and Monitoring |
| Parameter au-10: actions including the addition, modification, deletion, approval, sending, or receiving of data, including actions defined by DoDI 8520.02 and DoDI 8520.03 |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AU-10 What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for enforcing non-repudiation for customer-deployed resources.  **Azure**  As part of the content of audit records captured within Azure, unique identifiers are captured by servers, network devices, and services. Azure requires unique identifiers assigned based on individual’s unique account for Active Directory federation with domain and Authentication, Authorization, and Accounting (AAA) credentials. The combination of event logs capturing identifiers, and identifiers uniquely identified based on individual’s Azure accounts, constitute non-repudiation for the Azure environment.  For both Windows and Linux assets, the security logs are protected from non-repudiation and tampering using the following configurations, with the implementation being platform specific:  \* On the asset, Geneva Monitoring Agent (MA) authenticates from the asset to the central service for uploading security logs. The security logs use the Geneva Control-Plane Service (GCS) to manage the authentication from the agent on the asset to the Geneva Monitoring service. GCS uses an Azure Storage Shared Access Signatures (SAS) key implementation so that the full key is not exposed to the users on the asset.  \* The Azure service OpenTelemetry Audit logs and key system application security events such as anti-malware, PowerShell command line, and Terminal Services Remote Desktop Protocol access are uploaded every ten (10) minutes off the asset. The Linux system security event logs via AuditD and key system application security events such as anti-malware are uploaded every one (1) minute off the asset. The MA watermarks the system security and OpenTelemetry Audit events to confirm that events are uploaded. The configuration has retry values in case the central store is offline so that the MA continues to retry uploads of the events when connectivity is re-established.  \* Once the logs are uploaded to the Geneva Monitoring storage accounts for each service, the logs are submitted to downstream detection services within approximately fifteen (15) minutes to analyze specified security events for unusual activity. Analysis timelines vary depending on the type of detection. Additionally, the security logs are moved to cold storage every five (5) minutes as part of Geneva Monitoring.  \* Malicious activity on the asset that attempts to affect security log collection is monitored and alerted for, including monitoring for clearing of the security event log and audit policy changes. |

## AU-11 Audit Record Retention

Retain audit records for [a time period in compliance with M-21-31] to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements.

Requirement: The service provider retains audit records on-line for at least ninety days and further preserves audit records off-line for a period that is in accordance with NARA requirements.

Requirement: The service provider must support Agency requirements to comply with M-21-31 (https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-31-Improving-the-Federal-Governments-Investigative-and-Remediation-Capabilities-Related-to-Cybersecurity-Incidents.pdf)

Guidance: The service provider is encouraged to align with M-21-31 where possible

|  |
| --- |
| **AU-11 Control Summary Information** |
| Responsible Roles: Logging and Monitoring, Storage |
| Parameter au-11: at least one (1) year |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AU-11 What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for retaining audit records for customer-deployed resources to support security investigations and meet regulatory requirements. Audit records must be retained for the defined frequency.  **Azure**  Azure retains collected logs in storage for at least ninety (90) days to support investigations of security incidents and to meet regulatory retention requirements. Azure stores audit logs offline for at least one (1) year within Kusto storage.  C+AI Security has developed an archiving infrastructure to securely store audit records on servers dedicated to archival purposes. The servers are designed to verify the integrity of archived files and allows authorized user to browse to an archive location. Audit records are stored in centralized log servers that are protected against alteration. |

## AU-12 Audit Record Generation

a. Provide audit record generation capability for the event types the system is capable of auditing as defined in [AU-2a](#au-2\_smt.a) on [all information system and network components where audit capability is deployed/available];

b. Allow [personnel or roles allowed to select the event types that are to be logged by specific components of the system is/are defined;] to select the event types that are to be logged by specific components of the system; and

c. Generate audit records for the event types defined in [AU-2c](#au-2\_smt.c) that include the audit record content defined in [AU-3](#au-3).

|  |
| --- |
| **AU-12 Control Summary Information** |
| Responsible Roles: Logging and Monitoring, SDL |
| Parameter au-12\_odp.01: all information system components where audit capability is deployed |
| Parameter au-12\_odp.02: Azure Service Teams |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AU-12 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for ensuring all customer-deployed resources have the ability to generate records for the auditable events defined in AU-02.a.  **Azure**  Azure implements audit generation by configuring all servers, network devices, and services to have the capability to generate audit records and audit record metadata as required. Azure sets standard configuration baselines for all servers and network devices, ensuring the consistent generation of the required audit logs. Service teams ensure the required audit logs are captured at the service layer through the Azure Security Development Lifecycle (SDL) process. Azure also utilizes Azure Security Pack (AzSecPack), OpenTelemetry Audit, and Geneva Monitoring to ensure the central ingestion of those logs. |
| **Part B**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for assigning personnel to select audit events for customer-deployed resources.  **Azure**  Azure implements audit generation by configuring all system network devices and servers to have the capability to generate audit records and audit record metadata as required. Service teams configure audit generation for the service layer to generate audit records and audit record metadata as required. |
| **Part C**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for generating audit records for the subset of auditable events identified in AU-02.c and content defined in AU-03 for customer-deployed resources.  **Azure**  All Azure assets are required to generate audit records and audit record metadata as required. Audit records are captured in Geneva Monitoring, which allows for the record generation and reporting capabilities for the required auditable events. These capabilities also allow for the review of audit logs, should information contained within warrant a review. |

### AU-12(1) - System-wide and Time-correlated Audit Trail

Compile audit records from [all network, data storage, and computing devices] into a system-wide (logical or physical) audit trail that is time-correlated to within [level of tolerance for the relationship between timestamps of individual records in the audit trail is defined;].

|  |
| --- |
| **AU-12(1) Control Summary Information** |
| Responsible Roles: Logging and Monitoring |
| Parameter au-12.01\_odp.01: all network, data storage, and computing devices |
| Parameter au-12.01\_odp.02: one (1) millisecond |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AU-12(1) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for compiling audit records into a system-wide audit trail for customer-deployed resources.  **Azure**  Azure Security correlates audit logs across Azure using time stamps that are precise at least to the millisecond. The audit records are captured in Geneva Monitoring, which allows for the convergence of monitoring data for the required auditable events. To provide a time-correlated audit trail, all Azure logs are time correlated and stored in UTC time format. The time settings allow for a system-wide logical audit trail that is time-correlated to within one millisecond. |

### AU-12(3) - Changes by Authorized Individuals

Provide and implement the capability for [service provider-defined individuals or roles with audit configuration responsibilities] to change the logging to be performed on [all network, data storage, and computing devices] based on [selectable event criteria with which change logging is to be performed are defined;] within [time thresholds in which logging actions are to change is defined;].

|  |
| --- |
| **AU-12(3) Control Summary Information** |
| Responsible Roles: Logging and Monitoring |
| Parameter au-12.03\_odp.01: Azure Security; service team personnel with audit configuration responsibilities; Security Incident Monitoring Team |
| Parameter au-12.03\_odp.02: all network, data storage, and computing devices |
| Parameter au-12.03\_odp.03: changes to the threat environment; risk-based assessment defined in AU-02 |
| Parameter au-12.03\_odp.04: risk-based assessment; annually or whenever a change occurs in the threat environment as defined by authoritative sources from AU-02(03) |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **AU-12(3) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for providing the capability to extend or limit auditing on customer-deployed resources as necessary to meet organizational requirements.  **Azure**  The Azure Security Logging and Monitoring (SLAM) team and the Security Response Team have developed sets of auditable events for Azure assets based on ongoing risk assessments of the system which incorporate government and industry baselines and requirements, identified vulnerabilities, business requirements, and Azure and C+AI Security Standards. The event sets are reviewed by the SLAM and Security Response Team when a significant change to the system is made to ensure any vulnerabilities exposed are being addressed by the set of auditable events. New events are incorporated when a new asset class is brought online or when a vulnerability or threat is identified through security assessments, security bulletins, and more. The zero persistent access requirement through Just in Time (JIT) access also ensures that only authorized individuals are able to change the level of auditing on a given asset or at the AzSecPack layers. |

# Assessment, Authorization, and Monitoring (CA)

## CA-1 Policy and Procedures

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (OneOrMore): organization-level;mission/business process-level;system-level] assessment, authorization, and monitoring policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the assessment, authorization, and monitoring policy and the associated assessment, authorization, and monitoring controls;

b. Designate an [an official to manage the assessment, authorization, and monitoring policy and procedures is defined;] to manage the development, documentation, and dissemination of the assessment, authorization, and monitoring policy and procedures; and

c. Review and update the current assessment, authorization, and monitoring:

1. Policy [at least annually] and following [events that would require the current assessment, authorization, and monitoring policy to be reviewed and updated are defined;] ; and

2. Procedures [at least annually] and following [significant changes].

|  |
| --- |
| **CA-1 Control Summary Information** |
| Responsible Roles: SOP Team, Policy, Azure Compliance |
| Parameter ca-1(a): all personnel |
| Parameter ca-01\_odp.01: |
| Parameter ca-01\_odp.02: |
| Parameter ca-01\_odp.03: a Microsoft-wide |
| Parameter ca-01\_odp.04: the Microsoft Information Risk Management Council (IRMC) organization |
| Parameter ca-01\_odp.05: at least annually |
| Parameter ca-01\_odp.06: significant changes |
| Parameter ca-01\_odp.07: at least annually |
| Parameter ca-01\_odp.08: significant changes |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☒ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CA-1 What is the solution and how is it implemented?** |
| **Part A1**  **Customer Responsibility**  The customer is responsible for developing, documenting, and disseminating assessment, authorization, and monitoring policy and procedures that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.  **Azure**  Azure addresses the security assessment and authorization policy as part of the Microsoft security policies, of which there are two sets: the Microsoft Security Policy (MSP) that is applicable to all Microsoft personnel, and the Microsoft Security Program Policy (MSPP), which is applicable to all Microsoft personnel that have a responsibility for security. The Microsoft Information Risk Management Council (IRMC) is the governance body with review and approval responsibility for the MSP and MSPP. Within Azure, the MSPP specifically applies to all Microsoft personnel with security objectives such as, designing, building, and operating Azure and across all information and processes used in the conduct of Microsoft business . All Azure personnel are accountable and responsible for complying with these guiding principles within their designated roles. The policy addresses the following:  \* Compliance framework management  \* Organizational risk assessment  \* Information security coordination  \* Information security accountability  Additionally, the policy addresses the purpose, scope, roles, responsibilities, compliance requirements, and required coordination among the various Microsoft organizations that provide some level of support to all services. The policies indicate Microsoft management’s commitment and are a component of the risk management strategy which provides Azure personnel with a current set of clear and concise information security requirements.  The MSP is available to all Microsoft personnel on the Microsoft Policy website on the Microsoft intranet, and the MSPP and Security Standards are available through the Liquid tool, also on the Microsoft intranet. The Azure SOPs are stored in the Azure Security, Privacy & Compliance SharePoint site. This SharePoint site is accessible to all Azure personnel.  Service teams may supplement the Azure policies and procedures with offering-specific policies and procedures. Service-team-specific policies and procedures associated with security assessment and authorization are documented and stored within internal Azure SharePoint sites. Only personnel with authorized credentials, adequate levels of permission, legitimate need to know, and specific roles and responsibilities are given access to the service-team-specific policies or procedures. |
| **Part A2**  **Customer Responsibility**  The customer is responsible for procedures to facilitate the implementation of the assessment, authorization, and monitoring policy and the associated assessment, authorization, and monitoring controls.  **Azure**  The Azure Security Assessment and Authorization Standard Operating Procedure (SOP) implements the security assessment and authorization policy and associated controls and documents the following procedures:  \* Security assessments  \* Plan of action and milestones  \* Security authorization  \* Continuous monitoring  Service teams may supplement the Azure policies and procedures with offering-specific policies and procedures. Service-team-specific policies and procedures associated with security assessment and authorization are documented and stored within internal Azure SharePoint sites. Only personnel with authorized credentials, adequate levels of permission, legitimate need to know, and specific roles and responsibilities are given access to the service-team-specific policies or procedures. |
| **Part B**  **Customer Responsibility**  The customer is responsible for designating an official to manage the development, documentation, and dissemination of the assessment, authorization, and monitoring policy and procedures.  **Azure**  The Microsoft Information Risk Management Council (IRMC) organization is the governance body with approval responsibility for the Microsoft Security Policy (MSP) and Microsoft Security Program Policy (MSPP). The IRMC consists of representatives from security and risk management teams across Microsoft including Core Services Engineering and Operations (CSEO), Azure, and Global Security. The Customer Security and Trust: Security Engineering (CST-SE) organization manages the review and approval process and maintains the policies.  On an annual basis, the CST-SE conducts a line-by-line review of the MSP and MSPP. The Microsoft Security Policy (MSP) and Microsoft Security Program Policy (MSPP) Governance document describes each member’s role, types and frequency of review, escalation paths, approval process, and formal publishing procedures of the security policy. Throughout the year, if necessary, CST-SE may convene with the IRMC to conduct reviews after a significant review or change request. The approved policy update is published within the relevant tool on the Microsoft intranet. If service teams establish service-specific or team-specific policies, the respective service teams update the necessary policies at least annually. |
| **Part C1**  **Customer Responsibility**  The customer is responsible for reviewing and updating the current assessment, authorization, and monitoring policy on a regular basis and following organization defined events.  **Azure**  The Azure team updates the Azure SOPs at least annually through a formal review process. If needed, the Azure team updates the SOP after a significant change affecting policy execution as well. If established, service-team-specific procedures are updated by their respective teams. The individual service teams review and update their respective SOPs at least annually and when required by a significant change. |
| **Part C2**  **Customer Responsibility**  The customer is responsible for reviewing and updating the current assessment, authorization, and monitoring procedures on a regular basis and following organization defined events.  **Azure**  The Azure team updates the Azure SOPs at least annually through a formal review process. If needed, the Azure team updates the SOP after a significant change affecting policy execution as well. If established, service-team-specific procedures are updated by their respective teams. The individual service teams review and update their respective SOPs at least annually and when required by a significant change. |

## CA-2 Control Assessments

a. Select the appropriate assessor or assessment team for the type of assessment to be conducted;

b. Develop a control assessment plan that describes the scope of the assessment including:

1. Controls and control enhancements under assessment;

2. Assessment procedures to be used to determine control effectiveness; and

3. Assessment environment, assessment team, and assessment roles and responsibilities;

c. Ensure the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment;

d. Assess the controls in the system and its environment of operation [at least annually] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements;

e. Produce a control assessment report that document the results of the assessment; and

f. Provide the results of the control assessment to [individuals or roles to include FedRAMP PMO].

Guidance: Reference FedRAMP Annual Assessment Guidance.

|  |
| --- |
| **CA-2 Control Summary Information** |
| Responsible Roles: Azure Compliance |
| Parameter ca-02\_odp.01: at least annually |
| Parameter ca-02\_odp.02: at a minimum, the Azure ISSO/ISSM, FedRAMP PMO, the DISA A&A/SCA team, and the customer’s MCD |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CA-2 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  The customer is responsible for selecting the appropriate assessor or assessment team for the type of assessment to be conducted on customer-deployed resources.  **Azure**  Microsoft utilizes the Third Party Assessment Organization (3PAO) to conduct assessment against Azure clouds. |
| **Part B**  **Customer Responsibility**  The customer is responsible for developing a security assessment plan for the customer-deployed system. The assessment plan should address the scope of the assessment, including: controls and enhancements; assessment procedures; and the assessment environment, team, and roles/responsibilities.  **Azure**  Microsoft utilizes the Third Party Assessment Organization (3PAO) to develop a Security Assessment Plan (SAP) as part of the assessment performed for the Azure offering. The SAP addresses the following objectives:  \* Scope of the assessment  \* Assessment approach and methodology  \* Assessment environment  \* Known constraints, assumptions and dependencies that may impact the assessment effort  \* Required resources for performing the assessment  \* Assessment schedule  \* Guidelines for evaluating and reporting the assessment findings  \* Security controls and control enhancements under assessment  \* Assessment procedures to be used to determine security control effectiveness  The SAP is then reviewed and approved by Azure followed by a security assessment performed by the independent assessor. The SAP is based on NIST Special Publication 800-53A Revision 5. |
| **Part C**  **Customer Responsibility**  The customer is responsible for ensuring the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment for customer-deployed resources.  **Azure**  The SAP approved by Azure and Third Party Assessment Organization (3PAO) is reviewed and approved by the the FedRAMP JAB, DISA/DoD authorizing officials, and other regulators as required as necessary as a part of the security authorization package for an authorization decision. |
| **Part D**  **Customer Responsibility**  The customer is responsible for assessing the security controls defined in CA-02 on customer-deployed resources.  **Azure**  The assessment utilizes the SAP and the SSP as supporting documents to complete the security assessment and authorization activities in accordance with NIST Special Publication 800-37 Revision 2, which is used to serve as the basis for conducting security assessment and authorization activities for Azure. Azure conducts assessments at least on an annual basis. The assessment procedures are documented in NIST Special Publication 800-53A Revision 5, which also provides the assessment scope and frequency in combination with guidance from regulators. Assessment activities occur on an annual basis against the agreed-upon SAP between Microsoft, the Third Party Assessment Organization (3PAO), and authorizing officials. |
| **Part E**  **Customer Responsibility**  The customer is responsible for producing a security assessment report. The customer is also responsible for delivering the security assessment results to the required individuals/roles.  **Azure**  Upon completion of the security assessment, a Security Assessment Report (SAR) is developed by the Third Party Assessment Organization (3PAO) to document the results of security assessment and the risks associated with the system. The SAR documents the results of the assessment, including security controls that are considered other than satisfied, security control weaknesses, recommended remediation steps, and the risks associated with the system.  Azure and, if necessary, the 3PAO provide the SAR to the necessary authorizing officials including the FedRAMP JAB, DISA/DoD authorizing officials, and other regulators as required as necessary as a part of the security authorization package for an authorization decision. |
| **Part F**  **Customer Responsibility**  The customer is responsible for providing the results of control assessment to defined individuals or roles supporting customer-deployed resources.  **Azure**  The assessment utilizes the SAP and the SSP as supporting documents to complete the security assessment and authorization activities in accordance with NIST Special Publication 800-37 Revision 2, which is used to serve as the basis for conducting security assessment and authorization activities for Azure. Azure conducts assessments at least on an annual basis. The assessment procedures are documented in NIST Special Publication 800-53A Revision 5, which also provides the assessment scope and frequency in combination with guidance from regulators. Assessment activities occur on an annual basis against the agreed-upon SAP between Microsoft, the Third Party Assessment Organization (3PAO), and authorizing officials.  Azure and, if necessary, the 3PAO provide the SAR to the necessary authorizing officials including the FedRAMP JAB, DISA/DoD authorizing officials, and other regulators as required as necessary as a part of the security authorization package for an authorization decision. |

### CA-2(1) - Independent Assessors

Employ independent assessors or assessment teams to conduct control assessments.

Requirement: For JAB Authorization, must use an accredited 3PAO.

|  |
| --- |
| **CA-2(1) Control Summary Information** |
| Responsible Roles: Azure Compliance |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CA-2(1) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for employing independent assessors or assessment teams to conduct security control assessments.  **Azure**  Azure employs an approved Third Party Assessment Organization (3PAO) as an independent assessor to conduct a security control assessment of Azure in accordance with requirements. The results of this assessment and related activities are submitted to Azure’s authorizing officials. |

### CA-2(2) - Specialized Assessments

Include as part of control assessments, [at least annually], [Selection: announced;unannounced] , [Selection (OneOrMore): in-depth monitoring;security instrumentation;automated security test cases;vulnerability scanning;malicious user testing;insider threat assessment;performance and load testing;data leakage or data loss assessment;[other forms of assessment are defined (if selected);] ] .

Requirement: To include 'announced', 'vulnerability scanning'

|  |
| --- |
| **CA-2(2) Control Summary Information** |
| Responsible Roles: Azure Compliance |
| Parameter ca-02.02\_odp.01: at least annually |
| Parameter ca-02.02\_odp.02: announced |
| Parameter ca-02.02\_odp.03: vulnerability scanning and penetration testing |
| Parameter ca-02.02\_odp.04: |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CA-2(2) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for the selection of additional testing to be included as part of security control assessments.  **Azure**  The Third Party Assessment Organization (3PAO) assesses at least one third of all controls each year in accordance with continuous monitoring requirements, ensuring that all controls are assessed at least every three years. Other criteria, such as significant changes to the system or changes in risk posture and vulnerabilities, may trigger assessments.  The Third Party Assessment Organization (3PAO) performs penetration testing at least annually. The Penetration Test Report covers Azure system components identified as part of the authorization boundary. Additionally, in-depth monitoring is performed by the Security Response Team on a continuous basis as a part of incident management. The Third Party Assessment Organization (3PAO) also performs an independent validation of all vulnerability scanning conducted by Azure. |

### CA-2(3) - Leveraging Results from External Organizations

Leverage the results of control assessments performed by [any FedRAMP Accredited 3PAO] on [system on which a control assessment was performed by an external organization is defined;] when the assessment meets [the conditions of the JAB/AO in the FedRAMP Repository].

|  |
| --- |
| **CA-2(3) Control Summary Information** |
| Responsible Roles: Azure Compliance |
| Parameter ca-02.03\_odp.01: any FedRAMP Accredited 3PAO |
| Parameter ca-02.03\_odp.02: Azure |
| Parameter ca-02.03\_odp.03: the conditions of the JAB/AO in the FedRAMP Repository |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CA-2(3) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for accepting assessment results for customer-deployed resources.  **Azure**  Microsoft utilizes the Third Party Assessment Organization (3PAO) as an independent assessor to conduct a security control assessment of Azure and its components against the requirements of NIST Special Publication 800-53 Revision 5, Security and Privacy Controls for Federal Information Systems and Organizations. Azure accepts the results of the assessment from the 3PAO when the assessment meets the conditions of the Provisional ATO. The results of the assessment are documented in the SAR and submitted for authorizing official approval. |

## CA-3 Information Exchange

a. Approve and manage the exchange of information between the system and other systems using [Selection (OneOrMore): interconnection security agreements;information exchange security agreements;memoranda of understanding or agreement;service level agreements;user agreements;non-disclosure agreements;[the type of agreement used to approve and manage the exchange of information is defined (if selected);] ] ;

b. Document, as part of each exchange agreement, the interface characteristics, security and privacy requirements, controls, and responsibilities for each system, and the impact level of the information communicated; and

c. Review and update the agreements [at least annually and on input from JAB/AO].

|  |
| --- |
| **CA-3 Control Summary Information** |
| Responsible Roles: Azure Compliance |
| Parameter ca-03\_odp.01: interconnection security agreements, information exchange security agreements, memoranda of understanding or agreement, service level agreements, user agreements, nondisclosure agreements, or other agreements as appropriate |
| Parameter ca-03\_odp.02: |
| Parameter ca-03\_odp.03: at least annually and on input from JAB/AO |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CA-3 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  The customer is responsible for authorizing connections from the customer-deployed system to external systems using Interconnection Security Assessments.  **Azure**  Microsoft authorizes connections from the information system to other information systems outside of the authorization boundary through the use of vendor agreements, Memoranda of Understanding (MOUs), Interconnection Security Agreements (ISAs), Terms of Conditions (T&C), and/or Service Level Agreements (SLAs). Microsoft has developed the necessary vendor agreements, MOUs, ISAs, T&C, and SLAs that document connections outside of the Federal authorization boundary. Microsoft follows guidance regarding government agencies in that Interconnection Security Agreements (ISAs) are not designed for use between a CSP and Federal Agency. An Agency ATO memo should be the governing document for Agency and Azure interaction and security requirement communications. The only interconnections are between internal Microsoft services, which do not require ISAs.The internal Microsoft services that connect with Azure cloud are CorpNet and Cosmos. CorpNet is the Microsoft corporate network. CorpNet contains services run on Microsoft’s corporate network, not dedicated to Azure, such as source code repositories, system document repositories, and change ticketing. Cosmos is a service, not dedicated to Azure, that stores and reports on Azure log data. Microsoft Entra ID (formerly AAD) scrubs logs of customer information before sending logs to Cosmos.  At this time, Azure does not have any dependencies on information systems external to Microsoft that require ISAs. |
| **Part B**  **Customer Responsibility**  The customer is responsible for documenting the details of each interconnection defined in CA-03.a.  **Azure**  Azure Security is responsible for developing and maintaining MOU/ISA/T&C/SLA documents for Azure. These documents include the interface characteristics, security requirements and the nature of the information being communicated with third parties.  Azure documents in its MOU/ISA and T&C agreements with Microsoft services the interface characteristics, security requirements, information communicated, service requests, and service level agreements. These MOU/ISA and T&C documents serve as records between the Microsoft organizations of the commitments that were agreed to. Each document is signed by executive level Microsoft personnel who have responsibility over the systems interconnection. |
| **Part C**  **Customer Responsibility**  The customer is responsible for reviewing and updating Interconnection Security Agreements.  **Azure**  Microsoft monitors its Interconnection Security Agreements (ISAs) to verify security requirements. Microsoft conducts annual meetings with third parties to review agreements and any changes, and ensures that connection data described in ISAs is logged and monitored as part of the continuous monitoring process. Microsoft also reviews ISAs as needed, based on input from authorizing officials, and updates them when necessary. |

### CA-3(6) - Transfer Authorizations

Verify that individuals or systems transferring data between interconnecting systems have the requisite authorizations (i.e., write permissions or privileges) prior to accepting such data.

|  |
| --- |
| **CA-3(6) Control Summary Information** |
| Responsible Roles: Azure Compliance |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CA-3(6) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for verifying individuals or systems transferring data between interconnecting systems have the requisite authorizations prior to accepting such data on customer-deployed resources.  **Azure**  Currently, Azure does not have any connections to external information systems. The only interconnections are with internal Microsoft services. Azure authorizes connections from the information system to other information systems outside of the authorization boundary using vendor agreements, Memoranda of Understanding (MOUs), Interconnection Security Agreements (ISAs), Terms of Conditions (T&C), and/or Service Level Agreements (SLAs). Microsoft has developed the necessary vendor agreements, MOUs, ISAs, T&C, and SLAs that document connections outside of the Federal authorization boundary. Azure follows guidance regarding government agencies in that Interconnection Security Agreements (ISAs) are not designed for use between a CSP and Federal Agency. An Agency ATO memo should be the governing document for Agency and Azure interaction and security requirement communications. The only interconnections are between internal Microsoft services, which do not require ISAs. Personnel supporting internal Microsoft services are subject to background screening requirements during the Microsoft hiring process. Microsoft hiring managers work with Microsoft HR to ensure personnel are cleared through background screening before they are granted access to Microsoft systems. As such, personnel are authorized through the background screening processes validated by Microsoft hiring managers and Microsoft HR. Refer to control PS-03 for more details around background screening process. |

## CA-5 Plan of Action and Milestones

a. Develop a plan of action and milestones for the system to document the planned remediation actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system; and

b. Update existing plan of action and milestones [at least monthly] based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities.

Requirement: POA&Ms must be provided at least monthly.

Guidance: Reference FedRAMP-POAM-Template

|  |
| --- |
| **CA-5 Control Summary Information** |
| Responsible Roles: Continuous Monitoring |
| Parameter ca-5(b): at least monthly |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CA-5 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  The customer is responsible for developing a plan of action and milestones (POA&M) for customer-deployed resources. The POA&M should include planned remedial actions to correct deficiencies noted during the security assessment and to reduce/eliminate known vulnerabilities in the system. Additionally, any vulnerabilities found as a result of regular vulnerability scanning must be included in POA&M reporting.  **Azure**  Microsoft develops and maintains plans of action and milestones (POA&Ms) in accordance with Office of Management and Budget guidance and certification requirements. Microsoft updates the POA&M report monthly when vulnerability scans are run and any new vulnerabilities are identified, annually during security assessments, and as needed as a part of continuous monitoring activities. The POA&M is submitted as part of the Security Authorization Package provided to the authorizing officials. |
| **Part B**  **Customer Responsibility**  The customer is responsible for updating POA&M items defined in CA-05 Part a, which should include findings from security assessments, impact analyses, and continuous monitoring activities.  **Azure**  Microsoft updates the POA&M report on at least a monthly basis based on the findings of the security control assessments and ongoing continuous monitoring activities, including vulnerability scanning, utilizing an automated ConMon tool that tracks all open POA&Ms. Microsoft includes an action step to remediate any items from ongoing assessments and vulnerability scans (if any) consistent with the vulnerability management process in the monthly POA&M submission. Microsoft provides a high-level description of the issue and the remediation plan. The raw scan reports contain details on any issues noted and is made available to the authorizing officials monthly. |

## CA-6 Authorization

a. Assign a senior official as the authorizing official for the system;

b. Assign a senior official as the authorizing official for common controls available for inheritance by organizational systems;

c. Ensure that the authorizing official for the system, before commencing operations:

1. Accepts the use of common controls inherited by the system; and

2. Authorizes the system to operate;

d. Ensure that the authorizing official for common controls authorizes the use of those controls for inheritance by organizational systems;

e. Update the authorizations [in accordance with OMB A-130 requirements or when a significant change occurs].

(e) Guidance: Significant change is defined in NIST Special Publication 800-37 Revision 2, Appendix F and according to FedRAMP Significant Change Policies and Procedures. The service provider describes the types of changes to the information system or the environment of operations that would impact the risk posture. The types of changes are approved and accepted by the JAB/AO.

|  |
| --- |
| **CA-6 Control Summary Information** |
| Responsible Roles: Azure Compliance |
| Parameter ca-6(e): in accordance with OMB A-130 requirements or when a significant change occurs |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CA-6 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  The customer is responsible for assigning a senior authorizing official (AO) for customer-deployed resources.  **Azure**  Assessment and authorization activities follow established Federal processes as documented in NIST Special Publication 800-37 Revision 2, Guide for Applying the Risk Management Framework to Federal Information Systems. As part of the Security Authorization process, the authorizing officials review the Azure Security Authorization package to understand the level of risk posed by vulnerabilities identified in the information system and determine whether to grant a provisional ATO. The explicit acceptance of the risk to customer agency operations, assets, and individuals is the responsibility of customer organizations. The customer must consider many factors, balancing security considerations with mission and operational needs. The customer issues an authorization decision for the information system after reviewing the authorization package submitted by the Azure System Owner. The authorization package provides the FedRAMP JAB, DISA/DoD authorizing officials, other regulators, and customers with the essential information needed to make a credible risk-based decision on whether to grant a P-ATO for the offerings and services that comprise Azure. |
| **Part B**  **Customer Responsibility**  The customer is responsible for assigning a senior official as the authorizing official for common controls available for inheritance for customer-deployed resources.  **Azure**  Assessment and authorization activities follow established Federal processes as documented in NIST Special Publication 800-37 Revision 2, Guide for Applying the Risk Management Framework to Federal Information Systems. The Microsoft system does not inherit security controls from other systems. As part of the Security Authorization process, the authorizing officials review the Azure Security Authorization package for common controls available for inheritance to understand the level of risk posed by vulnerabilities identified in the information system and determine whether to grant a provisional ATO. The explicit acceptance of the risk to customer agency operations, assets, and individuals is the responsibility of customer organizations. The customer must consider many factors, balancing security considerations with mission and operational needs. The customer issues an authorization decision for the information system after reviewing the authorization package submitted by the Azure System Owner. The authorization package provides the FedRAMP JAB, DISA/DoD authorizing officials, other regulators, and customers with the essential information needed to make a credible risk-based decision on whether to grant a P-ATO for the offerings and services that comprise Azure. |
| **Part C**  **Customer Responsibility**  The customer is responsible for ensuring customer-deployed resources are authorized before operations commence.  **Azure**  The FedRAMP JAB, DISA/DoD authorizing officials, and other regulators determine if the remaining known vulnerabilities in the information system pose an acceptable level of risk to issue a P-ATO. Agencies must also determine whether the risk to agency operations, assets, and individuals is acceptable. Following review of the security authorization package and consultation with key agency officials, the FedRAMP JAB, DISA/DoD authorizing officials, and other regulators render an authorization decision to:  \* Authorize system operation without any restrictions or limitations on its operation;  \* Authorize system operation with restriction or limitation on its operation. The POA&M must be included detailed corrective actions to correct deficiencies. Resubmit an updated accreditation package upon completion of required POA&M actions to move to authorization to operate without any restrictions; or  \* Not authorize the system for operation. |
| **Part D**  **Customer Responsibility**  The customer is responsible for ensuring the authorizing official for common controls authorizes the use of those controls for inheritance by organizational systems.  **Azure**  The Microsoft system does not inherit security controls from other systems. The FedRAMP JAB, DISA/DoD authorizing officials, and other regulators determine if the remaining known vulnerabilities in the information system pose an acceptable level of risk to issue a P-ATO. Agencies must also determine whether the risk to agency operations, assets, and individuals is acceptable. Following review of the security authorization package and consultation with key agency officials, the FedRAMP JAB, DISA/DoD authorizing officials, and other regulators render an authorization decision to:  \* Authorize system operation without any restrictions or limitations on its operation;  \* Authorize system operation with restriction or limitation on its operation. The POA&M must be included detailed corrective actions to correct deficiencies. Resubmit an updated accreditation package upon completion of required POA&M actions to move to authorization to operate without any restrictions; or  \* Not authorize the system for operation. |
| **Part E**  **Customer Responsibility**  The customer is responsible for updating the security authorization for customer-deployed resources.  **Azure**  The FedRAMP JAB, DISA/DoD authorizing officials, and other regulators update the security authorization as needed based on submissions by Microsoft driven by the regular reauthorization schedule every three years or when there is a significant change as defined in NIST Special Publication 800-37 Revision 2, Appendix F. |

## CA-7 Continuous Monitoring

Develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the organization-level continuous monitoring strategy that includes:

a. Establishing the following system-level metrics to be monitored: [system-level metrics to be monitored are defined;];

b. Establishing [frequencies at which to monitor control effectiveness are defined;] for monitoring and [frequencies at which to assess control effectiveness are defined;] for assessment of control effectiveness;

c. Ongoing control assessments in accordance with the continuous monitoring strategy;

d. Ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy;

e. Correlation and analysis of information generated by control assessments and monitoring;

f. Response actions to address results of the analysis of control assessment and monitoring information; and

g. Reporting the security and privacy status of the system to [to include JAB/AO] [Assignment: organization-defined frequency].

Requirement: Operating System, Database, Web Application, Container, and Service Configuration Scans: at least monthly. All scans performed by Independent Assessor: at least annually.

Requirement: CSOs with more than one agency ATO must implement a collaborative Continuous Monitoring (ConMon) approach described in the FedRAMP Guide for Multi-Agency Continuous Monitoring. This requirement applies to CSOs authorized via the Agency path as each agency customer is responsible for performing ConMon oversight. It does not apply to CSOs authorized via the JAB path because the JAB performs ConMon oversight.

Guidance: FedRAMP does not provide a template for the Continuous Monitoring Plan. CSPs should reference the FedRAMP Continuous Monitoring Strategy Guide when developing the Continuous Monitoring Plan.

|  |
| --- |
| **CA-7 Control Summary Information** |
| Responsible Roles: Continuous Monitoring |
| Parameter ca-7(g)-1: customers and the FedRAMP JAB/AO |
| Parameter ca-7(g)-2: at least monthly |
| Parameter ca-07\_odp.01: rate of closure/remediation of POA&Ms and high vulnerabilities |
| Parameter ca-07\_odp.02: a continuous frequency |
| Parameter ca-07\_odp.03: at least annually |
| Parameter ca-07\_odp.04: |
| Parameter ca-07\_odp.05: |
| Parameter ca-07\_odp.06: |
| Parameter ca-07\_odp.07: |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CA-7 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  The customer is responsible for developing a continuous monitoring strategy and implementing a continuous monitoring program for customer-deployed resources.  **Azure**  As part of the configuration management process, Microsoft performs a Security Impact Analysis (SIA) and Business Impact Analysis (BIA) for all significant changes. Deficiencies to the system are documented in the SSP and SAR that are included in the Security Authorization Package. As part of continuous monitoring, Azure documents such as the SSP, SAR, and POA&M are updated to reflect any newly identified or remediated security issues. Additionally, Microsoft tracks through closure all vulnerabilities identified using the vulnerability scanning processes described in RA-05. In addition, cloud services tagged in Azure compliance and security boundary are required to complete compliance onboarding requirements designed to ensure the utilization of common Azure processes and tooling for addressing security risks. |
| **Part B**  **Customer Responsibility**  The customer is responsible for continuously monitoring customer-deployed resources and performing supporting assessments of that monitoring activity.  **Azure**  Microsoft tracks the rate of closure of POA&M and vulnerability items continuously and reviews this data at least monthly. |
| **Part C**  **Customer Responsibility**  The customer is responsible for ongoing security assessments in accordance with the customer's continuous monitoring strategy.  **Azure**  Microsoft has designated a security assessment program to evaluate the ongoing effectiveness of security controls outlined in the Azure SSP. The Security Assessment Program includes the assessment of all controls identified as necessary. Additionally, recommended technical testing is performed to meet the continuous monitoring requirements identified. |
| **Part D**  **Customer Responsibility**  The customer is responsible for ongoing security status monitoring of the metrics defined in CA-07 Part a.  **Azure**  Any new deficiencies that are identified from the security control assessments are documented in the POA&M. The POA&M is continuously updated and used to report on the security state of the information system as part of monthly reviews. POA&M updates are provided to customers monthly, consistent with requirements. |
| **Part E**  **Customer Responsibility**  The customer is responsible for correlating and analyzing security-related information generated by assessments and monitoring of customer-deployed resources.  **Azure**  The Azure Continuous Monitoring team performs correlation and analysis of security-related information generated by assessments and monitoring, including vulnerability scan results, POA&M updates, and recurring control testing.  Vulnerabilities are assessed if they are actionable (i.e. requiring remediation), risk reduced, false positive, or risk accepted. Microsoft mitigates all discovered high-risk vulnerabilities within thirty (30) days, all moderate-risk vulnerabilities within ninety (90) days, and all low-risk vulnerabilities within one hundred and eighty (180) days. The results are summarized into the Continuous Monitoring Reports and are input into the POA&M for tracking if applicable. |
| **Part F**  **Customer Responsibility**  The customer is responsible for responding to the results of the analysis defined in CA-07 Part e.  **Azure**  The Azure Continuous Monitoring team tracks open POA&Ms and vulnerabilities and coordinates with the service teams to drive these issues to closure. |
| **Part G**  **Customer Responsibility**  The customer is responsible for reporting the security status of customer-deployed resources.  **Azure**  Any new deficiencies that are identified from the security control assessments are documented in the POA&M. The POA&M is continuously updated and used to report on the security state of the information system as part of monthly reviews. POA&M updates are reviewed and validated by the Third Party Assessment Organization (3PAO), and are provided to customers and the FedRAMP JAB, DISA/DoD authorizing officials, and other regulators monthly, consistent with requirements. |

### CA-7(1) - Independent Assessment

Employ independent assessors or assessment teams to monitor the controls in the system on an ongoing basis.

|  |
| --- |
| **CA-7(1) Control Summary Information** |
| Responsible Roles: Azure Compliance |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CA-7(1) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for employing independent assessors or assessment teams to monitor security controls for customer-deployed resources on an ongoing basis.  **Azure**  Microsoft employs an independent assessment team to monitor security controls during monthly continuous monitoring activities and annually during the annual assessment. Microsoft utilizes an approved 3PAO to perform this monitoring, as well as to assess significant changes such as the addition of datacenters to the authorization boundary. |

### CA-7(4) - Risk Monitoring

Ensure risk monitoring is an integral part of the continuous monitoring strategy that includes the following:

(a) Effectiveness monitoring;

(b) Compliance monitoring; and

(c) Change monitoring.

|  |
| --- |
| **CA-7(4) Control Summary Information** |
| Responsible Roles: Azure Compliance, Continuous Monitoring |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CA-7(4) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for ensuring risk monitoring is an integral part of the continuous monitoring strategy which includes effectiveness, compliance, and change monitoring for customer-deployed resources.  **Azure**  Azure has designated a security assessment program to evaluate the ongoing effectiveness of security controls outlined in the Azure SSP as part of organizational defined continuous monitoring strategy. The Security Assessment Program includes the assessment of all controls identified in the High controls baseline of NIST SP 800-53 Revision 5, and recommended Security Controls for Information Systems and Organizations. Risk category is allocated to the security controls and controls deemed as core are tested on an annual basis by independent auditors and reviewed subsequently by Joint Authorization Board (JAB) of FedRAMP. Non-core controls are tested once every three years as determined by guidelines posed by the JAB. All controls are tested by independent auditors for effectiveness. Controls deemed not effective are allocated Plan of Action & Milestones (POA&Ms). Azure has a mature continuous monitoring program designed to track all identified POA&Ms. Risk categorization is applied on all POA&Ms and an analysis is done to ensure that appropriate mitigating factors/remediation steps are in place to address the risk of the POA&Ms. On a monthly cadence, POA&M reports are delivered to stakeholders of the security assessment program including independent auditors and the JAB. The mature Azure continuous monitoring program follows requirements posed by the JAB. The annual security assessment and continuous monitoring programs also bake in compliance and change monitoring whereby security controls are tested on an annual basis and identified POA&M are tracked continuously with monthly reporting to program stakeholders. Refer to CA-02 and CA-07 controls for more details on the programs. |

## CA-8 Penetration Testing

Conduct penetration testing [at least annually] on [systems or system components on which penetration testing is to be conducted are defined;].

Guidance: Reference the FedRAMP Penetration Test Guidance.

|  |
| --- |
| **CA-8 Control Summary Information** |
| Responsible Roles: Azure Compliance |
| Parameter ca-08\_odp.01: at least annually |
| Parameter ca-08\_odp.02: all information systems |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CA-8 What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for conducting penetration testing for customer-deployed resources.  **Azure**  An independent penetration testing team within Microsoft’s security organization conducts annual unannounced penetration testing. Tests may be coordinated with Azure management personnel in order to mitigate risk to the availability of Azure; Azure management personnel do not notify operational/technical personnel in these cases during the initial phase of the penetration testing execution.  As part of the rules of engagement, the Third Party Assessment Organization (3PAO) conducts a vulnerability analysis of the information system and penetration testing based on those results, as identified in the Security Assessment Report (SAR). The analysis steps are as follows:  \* The Third Party Assessment Organization (3PAO) reviews the Azure system security plan to determine if the required elementsas identified in NIST Special Publication 800-18 Revision 1 were properly documented.  \* The Third Party Assessment Organization (3PAO) reviews the Azure system security plan and related component documentation in order to determine if the security controls meet minimum security level recommendations.  \* The Third Party Assessment Organization (3PAO) reaches a consensus to perform the level and detail of testing for the system using assessment test cases and conducting an analysis to determine risk factors and impact.  \* The security assessment tests are designed to evaluate the efficacy of the security controls in place as documented in the system security plan to ensure that the levels of confidentiality, integrity, and availability are in fact supported by the existing in-place or proposed security measures or efforts.  \* The Third Party Assessment Organization (3PAO) develops and approves the Security Assessment Plan, and employs technical and non-technical measures to include, but not limited to, on-site interviews, observations, system testing, and evaluation.  \* The results of the assessment activities performed by the Third Party Assessment Organization (3PAO) include a formal report, which includes work papers that support the conclusions of the security assessment report.  \* Microsoft provides an exit brief of results, after the execution phase of the penetration testing is complete and prior to report finalization.  In addition to the annual penetration test conducted by an external party, Microsoft employs Red Team penetration test activities regularly. This testing is executed with approved penetration testing tools utilized by adversaries to ensure Azure is sufficiently tested against real-world attacks. |

### CA-8(1) - Independent Penetration Testing Agent or Team

Employ an independent penetration testing agent or team to perform penetration testing on the system or system components.

|  |
| --- |
| **CA-8(1) Control Summary Information** |
| Responsible Roles: Azure Compliance |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CA-8(1) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for employing an independent agent or team to perform penetration testing on customer-deployed resources (note that this may be the 3PAO used for recurring assessments, or it may be a different independent assessor).  **Azure**  The Third Party Assessment Organization (3PAO) performs penetration testing on the information system at least annually. The Penetration Test Report covers Azure system components identified as part of the authorization boundary. |

### CA-8(2) - Red Team Exercises

Employ the following red-team exercises to simulate attempts by adversaries to compromise organizational systems in accordance with applicable rules of engagement: [red team exercises to simulate attempts by adversaries to compromise organizational systems are defined;].

Guidance: See the FedRAMP Documents page> Penetration Test Guidance https://www.FedRAMP.gov/documents/

|  |
| --- |
| **CA-8(2) Control Summary Information** |
| Responsible Roles: Azure Compliance, Incident Response |
| Parameter ca-08.02\_odp: regular internal and annual external red team exercises and penetration tests |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CA-8(2) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for employing organization-defined red team exercises to simulate attempts by adversaries to compromise organizational information systems in accordance with organization-defined rules of engagement.  **Azure**  Microsoft employs Red Team penetration test activities regularly. This testing is executed with approved penetration testing tools utilized by adversaries to ensure Azure is sufficiently tested against real-world attacks. Including capabilities such as Threat Intelligence, Digital Crime Unit, Cyber Defense Operations Center, and Service Security Teams, the Azure Red Team coordinates overt and covert activities to validate and strengthen the global Azure and sovereign infrastructures. In addition, the Third Party Assessment Organization (3PAO) penetration tests are part of the overall compliance certifications. |

## CA-9 Internal System Connections

a. Authorize internal connections of [system components or classes of components requiring internal connections to the system are defined;] to the system;

b. Document, for each internal connection, the interface characteristics, security and privacy requirements, and the nature of the information communicated;

c. Terminate internal system connections after [conditions requiring termination of internal connections are defined;] ; and

d. Review [at least annually] the continued need for each internal connection.

|  |
| --- |
| **CA-9 Control Summary Information** |
| Responsible Roles: Logging and Monitoring, Networking |
| Parameter ca-09\_odp.01: components added through standard configuration management processes |
| Parameter ca-09\_odp.02: when no longer needed or authorized |
| Parameter ca-09\_odp.03: at least annually |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CA-9 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for authorizing internal connections across customer-deployed resources (e.g., system connections to VMs).  **Azure**  As part of standard configuration management processes, Microsoft authorizes individual assets connected to the environment. Teams generate threat models and/or data flow diagrams which include details of components within and connected to the information system.  Microsoft does not connect any constituent components to the Azure environment other than assets provisioned within the environment boundary. Such assets are subsequently considered part of the Azure information system once connected. Azure assets are configured according to Azure baselines. |
| **Part B**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for documenting the details of each internal connection between the classes/resources defined in CA-09.a.  **Azure**  As part of standard configuration management processes, Microsoft documents interface characteristics and security requirements for individual assets connected to the environment. These documents go through privacy, compliance, and security reviews.  To request a change to the host-based firewall, the service team must populate a questionnaire, providing descriptions of the request, requirements, and justification for the change. Depending on the asset classification of data, descriptions may include data types, current compliance with data handling, and any risk assessment or threat analysis the Azure team has conducted in coordination with Privacy, Corporate, External, and Legal Affairs (CELA), or C+AI Security. The Azure team must also provide documentation to help C+AI Security Solutions assess operational risks (e.g. architecture and network diagrams, infrastructure threat models, etc.). |
| **Part C**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for terminating internal system connections after a specified condition.  **Azure**  Microsoft does not connect any constituent components to the Azure environment other than assets provisioned within the environment boundary. Such assets are subsequently considered part of the Azure information system once connected. Assets are validated as part of the configuration management process, which includes security compliance checks to ensure the components are validated as approved assets for Azure. Once reviewed, Azure assets or connections that are no longer deemed necessary are removed through the Microsoft change management process. |
| **Part D**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for reviewing the continued need for each internal connection.  **Azure**  The Microsoft Change Management Standard specifies that all substantial changes must be reassessed and require review by the change review committee. Where appropriate, a Post-Implementation Review (PIR) may confirm that the change has met its objectives and that there have been no unexpected side-effects. |

# Configuration Management (CM)

## CM-1 Policy and Procedures

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (OneOrMore): organization-level;mission/business process-level;system-level] configuration management policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the configuration management policy and the associated configuration management controls;

b. Designate an [an official to manage the configuration management policy and procedures is defined;] to manage the development, documentation, and dissemination of the configuration management policy and procedures; and

c. Review and update the current configuration management:

1. Policy [at least annually] and following [events that would require the current configuration management policy to be reviewed and updated are defined;] ; and

2. Procedures [at least annually] and following [significant changes].

|  |
| --- |
| **CM-1 Control Summary Information** |
| Responsible Roles: SOP Team, Policy |
| Parameter cm-1(a): all personnel |
| Parameter cm-01\_odp.01: |
| Parameter cm-01\_odp.02: |
| Parameter cm-01\_odp.03: a Microsoft-wide |
| Parameter cm-01\_odp.04: the Microsoft Information Risk Management Council (IRMC) organization |
| Parameter cm-01\_odp.05: at least annually |
| Parameter cm-01\_odp.06: significant changes |
| Parameter cm-01\_odp.07: at least annually |
| Parameter cm-01\_odp.08: significant changes |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☒ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CM-1 What is the solution and how is it implemented?** |
| **Part A1**  **Customer Responsibility**  The customer is responsible for developing, documenting, and disseminating configuration management policy and procedures that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.  **Azure**  Azure addresses the configuration management policy as part of the Microsoft security policies, of which there are two sets: the Microsoft Security Policy (MSP) that is applicable to all Microsoft personnel, and the Microsoft Security Program Policy (MSPP), which is applicable to all Microsoft personnel that have a responsibility for security. The Microsoft Information Risk Management Council (IRMC) is the governance body with review and approval responsibility for the MSP and MSPP. The MSPP specifically applies to all Microsoft personnel with security objectives such as designing, building, and operating Azure and across all information and processes used in the conduct of Microsoft business. All Azure personnel are accountable and responsible for complying with these guiding principles within their designated roles. The policy addresses the following:  \* Purpose of providing rules and requirements to applicable personnel  \* Scope covering properties and services  \* Roles and responsibilities for those involved with the policy  \* Management commitment through coordination with security organizations, property security groups, and Microsoft corporate functions  \* Compliance by requiring all employees to adhere to the policy and applicable standards and follow approved procedures  Additionally, the policy addresses the purpose, scope, roles, responsibilities, compliance requirements, and required coordination among the various Microsoft organizations that provide some level of support to all services. The standards indicate Microsoft management’s commitment and are a component of the risk management strategy which provides Azure personnel with a current set of clear and concise information security requirements.  The MSP is available to all Microsoft personnel on the Microsoft Policy website on the Microsoft intranet, and the MSPP and Security Standards are available through the Liquid tool, also on the Microsoft intranet. The Azure SOPs are stored in the Azure Security, Privacy & Compliance SharePoint site. This SharePoint site is accessible to all Azure personnel.  Service teams may supplement the Azure policies and procedures with offering-specific policies and procedures. Service-team-specific policies and procedures associated with configuration management are documented and stored within internal Azure SharePoint sites. Only personnel with authorized credentials, adequate levels of permission, legitimate need to know, and specific roles and responsibilities are given access to the service-team-specific policies or procedures. |
| **Part A2**  **Customer Responsibility**  The customer is responsible for procedures to facilitate the implementation of the configuration management policy and the associated configuration management controls.  **Azure**  Azure implements the configuration management policy and associated controls through the following documents:  \* Azure Security Baseline Governance Standard Operating Procedure (SOP)  \* Azure Asset Management Standard Operating Procedure (SOP)  \* Azure Hardware Change and Release Management Standard Operating Procedure (SOP)  \* Azure Software Change and Release Management Standard Operating Procedure (SOP)  \* Microsoft Change Management Standard  \* Microsoft Security Standards  \* Microsoft Online Services Baseline Security Configuration Document  They document the following configuration management procedures:  \* Change control documentation, maintenance, retention, and approvals  \* Configuration baselines  \* Component inventory  \* Configuration settings  \* Segregation of duties for change management activities  \* Asset classification  Service teams may supplement the Azure policies and procedures with offering-specific policies and procedures. Service-team-specific policies and procedures associated with configuration management are documented and stored within internal Azure SharePoint sites. Only personnel with authorized credentials, adequate levels of permission, legitimate need to know, and specific roles and responsibilities are given access to the service-team-specific policies or procedures. |
| **Part B**  **Customer Responsibility**  The customer is responsible for designating an official to manage the development, documentation, and dissemination of the configuration management policy and procedures.  **Azure**  The Microsoft Information Risk Management Council (IRMC) organization is the governance body with approval responsibility for the Microsoft Security Policy (MSP) and Microsoft Security Program Policy (MSPP). The IRMC consists of representatives from security and risk management teams across Microsoft including Core Services Engineering and Operations (CSEO), Azure, and Global Security. The Customer Security and Trust: Security Engineering (CST-SE) organization manages the review and approval process and maintains the policies.  On an annual basis, the CST-SE conducts a line-by-line review of the MSP and MSPP. The Microsoft Security Policy (MSP) and Microsoft Security Program Policy (MSPP) Governance document describes each member’s role, types and frequency of review, escalation paths, approval process, and formal publishing procedures of the security policy. Throughout the year, if necessary, CST-SE may convene with the IRMC to conduct reviews after a significant review or change request. The approved policy update is published within the relevant tool on the Microsoft intranet. If service teams establish service-specific or team-specific policies, the respective service teams update the necessary policies at least annually. |
| **Part C1**  **Customer Responsibility**  The customer is responsible for reviewing and updating the current configuration management policy on a regular basis and following organization defined events.  **Azure**  The Azure team updates the Azure SOPs at least annually through a formal review process. If needed, the Azure team updates the SOP after a significant change affecting policy execution as well. If established, service-team-specific procedures are updated by their respective teams. The individual service teams review and update their respective SOPs at least annually and when required by a significant change. |
| **Part C2**  **Customer Responsibility**  The customer is responsible for reviewing and updating the current configuration management procedures on a regular basis and following organization defined events.  **Azure**  The Azure team updates the Azure SOPs at least annually through a formal review process. If needed, the Azure team updates the SOP after a significant change affecting policy execution as well. If established, service-team-specific procedures are updated by their respective teams. The individual service teams review and update their respective SOPs at least annually and when required by a significant change. |

## CM-2 Baseline Configuration

a. Develop, document, and maintain under configuration control, a current baseline configuration of the system; and

b. Review and update the baseline configuration of the system:

1. [at least annually and when a significant change occurs];

2. When required due to [to include when directed by the JAB] ; and

3. When system components are installed or upgraded.

(b)(1) Guidance: Significant change is defined in NIST Special Publication 800-37 Revision 2, Appendix F.

|  |
| --- |
| **CM-2 Control Summary Information** |
| Responsible Roles: Logging and Monitoring, Networking, SDL, Compute, Change Management, Privacy |
| Parameter cm-02\_odp.01: at least annually or when a significant change occurs |
| Parameter cm-02\_odp.02: JAB direction |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CM-2 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for developing, documenting, and maintaining a baseline configuration of customer-deployed resources. If the customer uses a non-Microsoft provided OS on Guest VMs, it is their responsibility to maintain and manage the baseline configuration on that OS. Additionally, it is the customer’s responsibility to maintain any application baselines they may have running in Azure.  **Azure**  Azure establishes and maintains configuration baselines using multiple sources, including:  \* Existing, updated, and new industry and regulator requirements  \* New software releases and configuration updates  \* Customer demand signals  \* External research findings and internal findings from incident management, penetration testing, security reviews, and other teams who are constantly learning about the operating environment  \* Compliance team requirements  Azure reviews and updates required configuration baselines at least annually. In all cases, changes to the configuration baselines are developed, tested, and approved prior to entering the production environment from a development or test environment. Configuration baselines are maintained under configuration control using Liquid, the Microsoft document repository.  Functionally, configuration baselines are reviewed and updated more often as a result of regular updates, reviews, and investigations. Logical images of the baselines are maintained in Azure DevOps. Azure applies configuration baselines differently for hardware and software: for hardware, using the bootstrap configuration process; for software, using the change and release process. Depending on the type of asset, there are different configuration baselines and processes.  **Servers**  Server configuration baselines are released and implemented internally via Azure Security Pack (AzSecPack). These configuration baselines are monitored by Azure Security Monitoring (ASM) and SCUBA using the baseline scanning component of AzSecPack. Supported versions of AzSecPack monitor both Windows and Linux operating systems. Additional supported operating systems versions and distributions are evaluated by the ASM team as part of semester planning twice a year and are then added based on business priority and resources.  **Azure Host, Azure Native, and Azure Guest Servers**  The RDOS team updates the server configuration baseline for Azure Host, Azure Native, and Azure Guest assets. The server base image is a version in which the kernel and many other core components have been modified to optimize them for the Azure environment. For service teams using Cloud Services, Windows server images are in the form of Virtual Hard Disks (VHDs) that are deployed as Guest VMs in the production environment. For Linux images, service teams use the Secure Base Image (SBI) that has been customized for secure configuration baselines relevant to Azure.  **Bare Metal and Pilotfish Servers**  The services running on Bare Metal and Pilotfish servers, including, but not limited to, Jumpboxes, Active Directory, Azure DNS, and other service teams, run standard Windows Server. The configuration baseline image for these assets is provided by the IPAK Engineering Team. IPAK incorporates the security configuration baselines established by the Azure Security Monitoring (ASM) team into the server images and makes those images available for consumption and deployment by engineering teams. Updated IPAK images are released monthly. IPAK documentation is made available to Microsoft personnel on the IPAK internal website, including release notes, install locations, and general IPAK information. Development changes to the IPAK are recorded, tested, and approved prior to implementation, as defined by the standardized change management process. The server is then configured per the role deployment specification by each service team, including the required validation steps prior to the server being released to production. The IPAK engineering team also manages deprecation of old baselines, notifying service team personnel at least twelve (12) months prior to end of life. Changes to the IPAK configurations are made only by appropriate personnel.  **Network Devices**  For network devices, the Azure Networking team sets the configuration baseline using recommended configurations specific to each hardware vendor, and makes updates periodically based upon recommendations from the vendor and internal analysis and investigation. For each type of network device, Azure Networking maintains configuration baseline documentation on the Azure Networking Standards and Architecture SharePoint site or in Azure DevOps. The networking configuration baselines are stored in Network Graph Database (NGS). Deployment methods, including reimaging, automated configuration update, scripted configuration change, and manual Method of Procedure (MOP) steps, call data from NGS. NGS provides a code-defined, source-controlled schema with the content to define the configuration baseline for each network device, meaning that the configuration on the device is generated from source regardless of the deployment method used. The network device configuration baseline itself is therefore stateless but the configuration generated from NGS data is, at any point in time, the Gold Configuration of that device. Only the Azure Networking team can make changes to configuration baselines for network devices in Azure.  When Azure Networking deploys network devices, the team runs the Config Policy Verifier (CPV) tool before the device goes live on the Azure production environment. CPV verifies the configuration of the device against the Gold Configuration of the appropriate device type. In addition, CPV runs ongoing daily monitoring of all network devices for conformance to the Gold Configuration.  **Azure Services**  Azure service teams maintain software assets running on the baselines described above. Each software asset has an established configuration baseline documented in code in a configuration file associated with the asset that is maintained under change control as part of the Change and Release Management processes. Service teams develop, document, and maintain the baselines for each asset in the approved software baseline repository, Azure DevOps. This ensures the baselines remain under configuration control. Changes to the code configuration baselines go through the Security Development Lifecycle (SDL) process, which requires approval from multiple individuals through Ownership Enforcer (OE) or branch policies prior to production deployment.  The configuration baseline for ports and protocols allowed for Azure services are monitored by the C+AI Security team via Network Isolation (NetIso). C+AI Security monitors network configurations of Windows and Linux services for internet-exposed management endpoints and high-risk ports and protocols as defined per the C+AI Platform security baseline process. |
| **Part B1**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for reviewing and updating the baseline configuration of customer-deployed resources.  **Azure**  Each configuration baseline team works with the respective imaging team for updates at least annually or when required due to a significant change and as part of new software or component-specific release and upgrade. Changes from United States Cyber Command tactical orders or directives can be accommodated. However, analysis is required to determine if a directive is applicable to the Azure services. There is a reasonable probability that a directive is not applicable. Microsoft internal components are specifically engineered for its operations and do not rely on third-party applications. They are further isolated from direct external connections. They must be further tested to ensure that there is no detrimental impact to the configuration baselines and that the associated vulnerability is not already accommodated by compensating or mitigating controls. All changes must go through the approved deployment process. Additionally, the configuration baselines may be reviewed and updated based on significant change to the Azure environment which may include, but is not limited to the following:  \* Adding new core missions or business functions  \* Acquiring specific and credible threat information that the organization is being targeted by a threat source  \* Establishing new or modified laws, directives, policies, or regulations  **Servers**  The Logging and Monitoring team thoroughly reviews and updates the Azure configuration baselines based on new security configurations or changes to existing security configurations of the OS and components at least annually or when a significant change occurs. Additionally, if business priorities require an update to the operating system image as part of the twice per year semester planning the baselines team works the respective imaging team - Azure RDOS team for Azure Host, Native, and Guest images, and IPAK for Bare Metal and Pilotfish - for updates as appropriate. Any updates to images are scheduled as part of the Change and Release Management process.  **Network Devices**  For network devices, the Azure Networking team sets the configuration baselines for network devices using recommended configurations specific to each vendor, and these teams make updates at least annually based upon recommendations from the vendors as well as internal testing, requirements, and feedback.  **Azure Services**  Azure utilizes a continuous integration and continuous deployment (CI/CD) model for services, ensuring the software baselines are updated regularly - in some cases, multiple times per day. Azure service teams maintain software baselines for each asset in the approved software baseline repository, Azure DevOps. This ensures the baselines remain under configuration control. Changes to configuration baselines go through the Security Development Lifecycle (SDL) process, which requires security signoffs prior to production deployment, among other security. |
| **Part B2**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for reviewing and updating the baseline configuration of customer-deployed resources when required by organization-defined circumstances.  **Azure**  Each configuration baseline team works with the respective imaging team for updates at least annually or when required due to a significant change. Changes from United States Cyber Command tactical orders or directives can be accommodated. However, analysis is required to determine if a directive is applicable to the Azure services. There is a reasonable probability that a directive is not applicable. Microsoft internal components are specifically engineered for its operations and do not rely on third-party applications. They are further isolated from direct external connections. They must be further tested to ensure that there is no detrimental impact to the configuration baselines and that the associated vulnerability is not already accommodated by compensating or mitigating controls. All changes must go through the approved deployment process. Additionally, the configuration baselines may be reviewed and updated based on significant change to the Azure environment which may include, but is not limited to the following:  \* Adding new core missions or business functions  \* Acquiring specific and credible threat information that the organization is being targeted by a threat source  \* Establishing new or modified laws, directives, policies, or regulations |
| **Part B3**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for reviewing and updating the baseline configuration of customer-deployed resources when installations and upgrades occur.  **Azure**  Each configuration baseline team works with the respective imaging team for updates as appropriate to applicable configuration baselines as part of the new software or component-specific release and upgrade. |

### CM-2(2) - Automation Support for Accuracy and Currency

Maintain the currency, completeness, accuracy, and availability of the baseline configuration of the system using [automated mechanisms for maintaining baseline configuration of the system are defined;].

|  |
| --- |
| **CM-2(2) Control Summary Information** |
| Responsible Roles: Logging and Monitoring, Networking, Change Management |
| Parameter cm-02.02\_odp: organization-defined automated mechanisms |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CM-2(2) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for employing automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of customer-deployed resources.  **Azure**  **Servers**  Configuration baseline information is stored in Azure DevOps, an automated tool that allow Azure to maintain an up-to-date, complete, accurate, and readily available configuration baseline of Azure assets.  **Network Devices**  All configuration baselines are stored as abstracted metadata in the network graph database (NGS). NGS is itself managed in a compliant and source-controlled instance of Azure DevOps.  **Azure Services**  Configuration baseline information as code is stored in Azure DevOps, an automated tool that allow Azure to maintain an up-to-date, complete, accurate, and readily available configuration baseline of Azure services. |

### CM-2(3) - Retention of Previous Configurations

Retain [organization-defined number of previous versions of baseline configurations of the previously approved baseline configuration of IS components] of previous versions of baseline configurations of the system to support rollback.

|  |
| --- |
| **CM-2(3) Control Summary Information** |
| Responsible Roles: Logging and Monitoring, Networking, Change Management |
| Parameter cm-02.03\_odp: the most recent previous version of the baseline configuration |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CM-2(3) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for retaining previous versions of baseline configurations for customer-deployed resources.  **Azure**  Azure implements procedures for at least the most recent previous version of the configuration baseline and configuration settings within at least one internal baseline storage solution, in the event services need to roll back to a stable version.  **Servers**  Configuration baselines and configuration settings are available via the Azure DevOps repository history in case a rollback to a previous baseline version is required. Additionally, a copy of the official configuration baseline is published internally to the Liquid requirements catalog that is the authoritative source of requirements authored and maintained by Corporate, External and Legal Affairs (CELA) policy owners as well as other groups across the company.  **Network Devices**  Previous versions of the configuration baselines for network devices are maintained permanently and archived in Network Device Manager (NDM) for at least three (3) months. Network Device Manager is a Microsoft-built software for storing configuration templates. In addition, networking configuration baselines are stored in Network Graph Database (NGS) and Azure DevOps indefinitely.  **Azure Services**  Service code is stored in Azure DevOps, which retains older versions of code indefinitely. |

### CM-2(7) - Configure Systems and Components for High-risk Areas

(a) Issue [the systems or system components to be issued when individuals travel to high-risk areas are defined;] with [configurations for systems or system components to be issued when individuals travel to high-risk areas are defined;] to individuals traveling to locations that the organization deems to be of significant risk; and

(b) Apply the following controls to the systems or components when the individuals return from travel: [the controls to be applied when the individuals return from travel are defined;].

|  |
| --- |
| **CM-2(7) Control Summary Information** |
| Responsible Roles: Azure Compliance |
| Parameter cm-02.07\_odp.01: Not applicable |
| Parameter cm-02.07\_odp.02: Not applicable |
| Parameter cm-02.07\_odp.03: Not applicable |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☒ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☒ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CM-2(7) What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  The customer is responsible for mobile devices within their environment.  **Azure**  Azure customer content is never stored outside of Azure, which is physically located within the continental United States. Azure personnel do not travel with devices contained within the Azure inventory. |
| **Part B**  **Customer Responsibility**  The customer is responsible for mobile devices within their environment.  **Azure**  Azure customer content is never stored outside of Azure, and Azure personnel do not travel with devices contained within the Azure inventory. |

## CM-3 Configuration Change Control

a. Determine and document the types of changes to the system that are configuration-controlled;

b. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses;

c. Document configuration change decisions associated with the system;

d. Implement approved configuration-controlled changes to the system;

e. Retain records of configuration-controlled changes to the system for [the time period to retain records of configuration-controlled changes is defined;];

f. Monitor and review activities associated with configuration-controlled changes to the system; and

g. Coordinate and provide oversight for configuration change control activities through [the configuration change control element responsible for coordinating and overseeing change control activities is defined;] that convenes [Selection (OneOrMore): [the frequency at which the configuration control element convenes is defined (if selected);] ;when [configuration change conditions that prompt the configuration control element to convene are defined (if selected);] ] .

Requirement: The service provider establishes a central means of communicating major changes to or developments in the information system or environment of operations that may affect its services to the federal government and associated service consumers (e.g., electronic bulletin board, web status page). The means of communication are approved and accepted by the JAB/AO.

(e) Guidance: In accordance with record retention policies and procedures.

|  |
| --- |
| **CM-3 Control Summary Information** |
| Responsible Roles: Logging and Monitoring, Networking, SDL, Compute, Change Management, Privacy |
| Parameter cm-03\_odp.01: at least ninety (90) days |
| Parameter cm-03\_odp.02: oversight committee or crossgroup review |
| Parameter cm-03\_odp.03: monthly, or as needed; major change |
| Parameter cm-03\_odp.04: |
| Parameter cm-03\_odp.05: |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CM-3 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for determining what types of changes to customer-deployed resources are configuration-controlled.  **Azure**  Configuration baselines are established based on industry standards, including CIS Benchmarks, DISA STIGs, NSA, various vulnerability library knowledgebases that are configuration related, and vendor recommendations. Configuration baselines undergo through review by security settings baseline experts within Azure, including the Security Assurance team and Microsoft Security Response Center, and other baseline experts across other Microsoft divisions who participate in a Shared Baselines working group. The industry standards and input from baseline experts across Microsoft along with the environment-specific considerations and some role- or instance-specific settings are used to establish the configuration settings. Changes to configuration baselines are handled through the update process at least annually, but also when new asset types are added to the inventory.  Changes to operational services can only be made when there is a valid business reason such as a planned upgrade to the service. Changes implemented within the production environment are categorized into Request for Change (RFC) types to appropriately schedule, align resources, and provide change metrics back into the change process for continuous improvement. Azure service teams use the following RFC types: Major Release, Minor Release, and Revision Release. Naming convention for build releases varies by service teams and the specific processes required for the release are specified in the service team specific change management process documents.  Changes to configuration settings on Azure assets are handled in two ways. Code changes, image updates, and network device gold images follow the Microsoft Security Development Lifecycle (SDL) process, which requires approval from multiple individuals through Ownership Enforcer (OE) or branch policies prior or branch policies to production deployment. Changes to the configuration settings are deployed to the production environment using the change and release management process, including mandatory Safe Deployment Practices (SDP). These processes validate that the configuration setting changes move from one environment to the other with designated signoff by appropriate Azure service team personnel. Access to migrate changes to production is restricted to the appropriate users via OneIdentity security groups.  Changes to configuration settings on running assets made through interactive means, such as logging into and changing a configuration setting of a Windows server, must be made through the standard access elevation process. Different assets have different protections in place, depending on the impact of the change.  **Servers**  Azure Security Monitoring (ASM) monitors for configuration setting changes. Service teams are able to make certain changes that are not security relevant without response or alerting, but if critical configuration settings, such as audit and log settings, are changed, the action generates an IcM ticket for remediation.  **Network Devices**  Any network device change not correlated with a work ticket will generate an IcM ticket for investigation and potential remediation. |
| **Part B**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for reviewing proposed configuration-controlled changes to customer-deployed resources.  **Azure**  All changes under configuration control to Azure assets are reviewed and approved or disapproved with explicit consideration for security and privacy impact analysis. Per the Microsoft Change Management Standard, all changes require documented testing procedures.  **Servers**  It is the responsibility of the change tester to verify against defined test and success criteria and to record the test results in the work item tracking the change. For IPAK changes, all work items impacting code are triaged by the IPAK team before they are implemented. The triage process assesses the priority of the item and potential impact to customers. If an item is of a security nature, input from C+AI Platform Security is sought. For RDOS changes, changes are tested in a non-production environment before being promoted to production. All changes go through the standard change management process which includes a security impact analysis.  **Network Devices**  Security impact analyses for network device changes are completed by performing a risk assessment for the change being performed. |
| **Part C**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for documenting configuration-controlled changes associated with customer-deployed resources (see CM-03.b).  **Azure**  Azure service teams use Azure DevOps or IcM for change management tracking, where source code and work items related to configuration baselines and configuration settings are tracked. Work items and source code changes document evidence of approvals and track all changes made to releasing a new configuration setting. |
| **Part D**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for implementing configuration-controlled changes approved in CM-03.b.  **Azure**  Azure DevOps ensures that configuration-controlled changes are implemented after they are approved by tracking the change through implementation. |
| **Part E**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for retaining a record of configuration-controlled changes to customer-deployed resources.  **Azure**  Depending on the type of change, the evidence of release approval is documented in either Azure DevOps or IcM. These change management records are retained for a minimum of ninety (90) days. |
| **Part F**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for auditing and reviewing configuration changes.  **Azure**  The tools outlined in Part c of this control provide an auditing capability to any changes to the configuration baselines or configuration settings within the tools. Microsoft uses Azure DevOps as the versioning system for Azure code, which tracks the identity of the Azure service team personnel who check code out, the time of the change, and what changes are made to what files. Software and hardware changes are tracked through Azure DevOps or IcM, which also provide detailed audit records of action taken. Deployment services including OneBranch also audit and centrally report actions taken. |
| **Part G**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for coordinating and providing oversight for configuration change control activities.  **Azure**  All changes to the Azure production environment, except pre-approved changes, must go thorough peer review, oversight committee review, or cross group review approval. How this is implemented depends on the team and the change to be introduced.  Changes to source code within the source code repository require a second approval from someone other than the submitter. This ensures that all source code changes are reviewed and the service team provides oversight of all changes when they are pushed into the production source code.  Changes to the production environment require a work ticket and JIT approval, ensuring that all changes are either reviewed manually via JIT or automatically via JIT auto-approval policies. There are a set of pre-approved changes which do not require additional explicit approval for release. These are standard procedures and common tasks that are documented and are confirmed to be safe to perform without going through the formal change management process. Examples of pre-approved Change Types are Create Certificate and Create Stage XStore Account.  For all Azure assets, Azure works with its authorizing officials by participating in regular meetings with the FedRAMP JAB, DISA/DoD authorizing officials, and other regulators and ISSOs as needed to communicate major changes to or developments in the Azure environment. |

### CM-3(1) - Automated Documentation, Notification, and Prohibition of Changes

Use [mechanisms used to automate configuration change control are defined;] to:

(a) Document proposed changes to the system;

(b) Notify [approval authorities to be notified of and request approval for proposed changes to the system are defined;] of proposed changes to the system and request change approval;

(c) Highlight proposed changes to the system that have not been approved or disapproved within [organization agreed upon time period];

(d) Prohibit changes to the system until designated approvals are received;

(e) Document all changes to the system; and

(f) Notify [organization defined configuration management approval authorities] when approved changes to the system are completed.

|  |
| --- |
| **CM-3(1) Control Summary Information** |
| Responsible Roles: Logging and Monitoring, Networking, Compute, Change Management |
| Parameter cm-03.01\_odp.01: organization-defined automated mechanisms |
| Parameter cm-03.01\_odp.02: authorized approvers, committee |
| Parameter cm-03.01\_odp.03: thirty (30) days |
| Parameter cm-03.01\_odp.04: service team management, personnel associated with the change |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CM-3(1) What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for employing automated mechanisms to document proposed changes (see CM-03.b).  **Azure**  Depending on the type of change, configuration setting changes are documented in either Incident Management (IcM) or Azure DevOps. These change management records are retained for a minimum of ninety (90) days. |
| **Part B**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for employing an automated mechanism to route and request approval for proposed changes to customer-deployed resources.  **Azure**  The IcM and DevOps automated tools used to track and document changes automatically notify the authorized approvers of proposed changes and request change approval. Records of changes are retained within tickets for all changes. |
| **Part C**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for employing an automated mechanism to highlight unreviewed change proposals.  **Azure**  The current queue of proposed changes is reviewed by the service team as part of regular review meetings at least monthly. Changes can be abandoned; this is a normal part of the change management lifecycle. |
| **Part D**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for employing an automated mechanism to prohibit the implementation of unapproved changes to customer-deployed resources.  **Azure**  All the change management tools prevent changes from being deployed without approval from an authorized approver. Interactive access via elevation to production assets requires separate approval or approval of properly configured auto-approval in the Just In Time (JIT) tool. |
| **Part E**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for employing an automated mechanism to document all implemented changes to customer-deployed resources.  **Azure**  All changes are tracked and documented within the appropriate automated change tracking system. Azure teams use tools such as Azure DevOps or IcM for documentation and tracking purposes. All assets implement auditing for changes made via interactive login. |
| **Part F**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for employing an automated mechanism to provide notifications when approved changes to customer-deployed resources are completed.  **Azure**  Upon successful deployment of a change, the relevant service team management personnel, including the change submitters and approvers, are automatically notified by the change tracking system. |

### CM-3(2) - Testing, Validation, and Documentation of Changes

Test, validate, and document changes to the system before finalizing the implementation of the changes.

|  |
| --- |
| **CM-3(2) Control Summary Information** |
| Responsible Roles: Logging and Monitoring, Networking, Compute, Change Management |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CM-3(2) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for testing, validating, and documenting changes to customer-deployed resources before implementation.  **Azure**  Each service team tests proposed system changes prior to deployment, either in a separate test environment, or by removing a server from production, making changes, testing, and returning the server to production upon successful completion. Azure implements safe deployment known as Safe Deployment Practices (SDP), which includes testing in canary regions and rolling out to increasing percentages of the applicable environment before considering the rollout complete. Azure assets have a set of runners which leverage information captured by Geneva Monitoring to run automated tests for checking the health of the components. Runners are configured to automatically generate alerts if any component health discrepancies are identified. This ensures recently deployed software should be propagated to more assets or rolled back as health indicators dictate. If there are any issues during the rollout, the deployment is halted to investigate.  All code impacting work items are triaged before they are implemented. The triage process assesses the priority of the item and potential impact to customers. If an item is of a security nature, input from C+AI Security is sought. Assets have a set of runners which leverage information captured by Geneva Monitoring to run automated tests for checking the health of the components. Runners are configured to automatically generate alerts if any component health discrepancies are identified. This ensures recently deployed software should be propagated to more assets or rolled back as health indicators dictate.  Testing procedures for changes are documented within change tickets. Configuration changes and associated approvals and documentation are all kept within tickets or RFC. Automation is built into the change management tool throughout the change lifecycle including documenting changes to the information system. |

### CM-3(4) - Security and Privacy Representatives

Require [Assignment: organization-defined security and privacy representatives] to be members of the [Configuration control board (CCB) or similar (as defined in CM-3)].

|  |
| --- |
| **CM-3(4) Control Summary Information** |
| Responsible Roles: Logging and Monitoring, Networking, Compute, Change Management |
| Parameter cm-3.4\_prm\_1: organization-defined security and privacy representatives |
| Parameter cm-03.04\_odp.01: |
| Parameter cm-03.04\_odp.02: |
| Parameter cm-03.04\_odp.03: committee |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CM-3(4) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for assigning an information security and privacy representative to be a member of the change control element defined in CM-03.g.  **Azure**  All changes, except pre-approved changes, to the Azure production environment must go through service team committee approval. Each service team has an internal committee with designated roles, and which include representatives from Azure Security; these meet at least monthly or as needed.  **Servers**  The C+AI Platform Security baseline team establishes and maintains the configuration baseline standards for operating systems and service network configurations. The baselines are established based on industry standards, including DISA STIGs, CIS, NSA, and various vulnerability library knowledge bases that are configuration related, and through review of security settings baseline experts within C+AI Platform Security including the Security Assurance team and Microsoft Security Response Center and other baseline experts across other Microsoft divisions who participate in the overall Shared Baselines Teams group virtual team. The industry standards and input from baseline experts across Microsoft along with the environment specific considerations and some role specific settings - e.g. domain controller, workgroup server, domain joined server - are used to establish the configuration settings. The Shared Baselines crossgroup includes required representatives from C+AI Platform Security including members from the Security Response Team and the Security Assurance team. Additionally, key participants include members from the incident response team and participants from Microsoft consulting who bring in field experience.  **Network Devices**  For network devices, the Azure Network Engineering teams sets the configuration baseline standards for all network devices, using recommended configurations specific to each hardware vendor including applicable STIGs, and makes updates periodically based upon recommendations from the vendor. For each type of device, the Azure Network Engineering teams maintains configuration baselines in Network Device Manager (NDM). Only the Azure Networking team can make changes to configuration baselines for network devices in the Azure environment. |

### CM-3(6) - Cryptography Management

Ensure that cryptographic mechanisms used to provide the following controls are under configuration management: [All security safeguards that rely on cryptography].

|  |
| --- |
| **CM-3(6) Control Summary Information** |
| Responsible Roles: Logging and Monitoring, Secret Management Stores |
| Parameter cm-03.06\_odp: all security controls that rely on cryptography |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CM-3(6) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for ensuring that cryptographic mechanisms are under configuration management.  **Azure**  Azure Security manages cryptographic secrets on behalf of service teams using an approved secret management store, either Azure Key Vault or dSMS. Microsoft uses the stores to implement cryptographic mechanisms, including to administer and store both group and shared account credentials, as well as to obtain and renew certificates. Cryptography changes follow the standard security review process. Cryptographic changes not expressly allowed by established baselines - e.g. when an Azure team requests a non-standard change to configuration settings - are not allowed to be made to the Azure current configuration without a completed review. The security review process is run by security representatives in C+AI Security. Changes made to cryptography are not implemented unless approved via the security review process including approval by Crypto Board.  Azure Security controls the configuration of the stores using the Cryptographic Controls Standard Operating Procedure (SOP), with which the stores are required to comply. For instance, when Microsoft deprecates formerly-approved cryptographic algorithms or key lengths through the change management process, the secret management stores are able to check the inventory of all existing secrets to identify any that rely on the newly-deprecated mechanism. |

## CM-4 Impact Analyses

Analyze changes to the system to determine potential security and privacy impacts prior to change implementation.

|  |
| --- |
| **CM-4 Control Summary Information** |
| Responsible Roles: Logging and Monitoring, Networking, SDL, Compute, Change Management, Privacy |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CM-4 What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for analyzing proposed changes to customer-deployed resources to determine potential security and privacy impacts prior to implementation.  **Azure**  As part of the Security Development Lifecycle (SDL) process, Azure analyzes software and hardware changes to determine potential security impacts prior to change implementation. Changes are required to be documented, tested, and approved by appropriate service team personnel. For all asset types, changes are analyzed as part of the standard change management process, both prior to and after implementation, to verify what was modified resulted in expected output.  The SDL process is followed for all engineering and development projects. The SDL process consists of five phases: Requirements, Design, Implementation, Verification and Release. The Requirements phase considers the foundational security, privacy, and cost requirements for a given product. The Design phase is the creation of the plan to implement the product to meet the defined requirements, including risk and threat model analysis. The implementation phase is when security documentation is created for the product, allowing users and customers to make informed decisions on how to deploy it, as well as initial testing to remove any security or privacy issues. The Verification phase is when the implementation is reviewed to ensure that the security and privacy tenets defined in the Requirements phase, and where full product testing takes place. Finally, the Release phase is the creation of incident planning, should any issues regarding the product arise once it is available.  Each service team tests proposed system changes prior to deployment, either in a separate test environment, or by removing a server from production, making changes, testing, and returning the server to production upon successful completion. Azure implements safe deployment known as Safe Deployment Practices (SDP), which includes testing in canary regions and rolling out to increasing percentages of the applicable environment before considering the rollout complete. Azure assets have a set of runners which leverage information captured by Geneva Monitoring to run automated tests for checking the health of the components. Runners are configured to automatically generate alerts if any component health discrepancies are identified. This ensures recently deployed software should be propagated to more assets or rolled back as health indicators dictate. If there are any issues during the rollout, the deployment is halted to investigate. |

### CM-4(1) - Separate Test Environments

Analyze changes to the system in a separate test environment before implementation in an operational environment, looking for security and privacy impacts due to flaws, weaknesses, incompatibility, or intentional malice.

|  |
| --- |
| **CM-4(1) Control Summary Information** |
| Responsible Roles: Logging and Monitoring, Networking, SDL, Compute, Change Management, Privacy |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CM-4(1) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for analyzing proposed changes to customer-deployed resources in a test environment before implementation in an operational environment to identify security and privacy impacts due to flaws, weaknesses, incompatibility, or intentional malice.  **Azure**  The Microsoft Security Development Lifecycle (SDL) process is followed for all engineering and development projects. The SDL process consists of five phases: Requirements, Design, Implementation, Verification, and Release. The Requirements phase considers the foundational security, privacy, and cost requirements for a given product. The Design phase is the creation of the plan to implement the product to meet the defined requirements, including risk and threat model analysis. The implementation phase is when security documentation is created for the product, allowing users and customers to make informed decisions on how to deploy it, as well as initial testing to remove any security or privacy issues. The Verification phase is when the implementation is reviewed to ensure that the security and privacy tenets defined in the Requirements phase, and where full product testing takes place. Finally, the Release phase is the creation of incident planning, should any issues regarding the product arise once it is available.  Each service team tests proposed system changes prior to deployment, either in a separate test environment, or by removing a server from production, making changes, testing, and returning the server to production upon successful completion. Azure implements safe deployment known as Safe Deployment Practices (SDP), which includes testing in canary regions and rolling out to increasing percentages of the applicable environment before considering the rollout complete. Azure assets have a set of runners which leverage information captured by Geneva Monitoring to run automated tests for checking the health of the components. Runners are configured to automatically generate alerts if any component health discrepancies are identified. This ensures recently deployed software should be propagated to more assets or rolled back as health indicators dictate. If there are any issues during the rollout, the deployment is halted to investigate. |

### CM-4(2) - Verification of Controls

After system changes, verify that the impacted controls are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security and privacy requirements for the system.

|  |
| --- |
| **CM-4(2) Control Summary Information** |
| Responsible Roles: Logging and Monitoring, Networking, Compute, Change Management |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CM-4(2) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for, after the information system is changed, checking the security functions to verify that the functions are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security and privacy requirements for the system.  **Azure**  Azure assets have a set of runners which leverage information captured by Geneva Monitoring to run automated tests for checking the health of the components. Runners are configured to automatically generate alerts if any component health discrepancies are identified. This ensures recently deployed software should be propagated to more assets or rolled back as health indicators dictate. If there are any issues during the rollout, the deployment is halted to investigate. Azure also performs periodic audit of the security functions to confirm their operating effectiveness via ASM. |

## CM-5 Access Restrictions for Change

Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.

|  |
| --- |
| **CM-5 Control Summary Information** |
| Responsible Roles: JIT, OneIdentity, Logging and Monitoring, Networking, Compute, Change Management |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CM-5 What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for enforcing logical access restrictions when making changes to customer-deployed resources.  **Azure**  Azure service teams define, document, approve, and enforce logical access restrictions associated with changes by using role-based access control (RBAC) enforced by Active Directory (AD). All accounts created in support of Azure are role-based. Service team personnel request access to, and if approved, are placed in the appropriate security groups according to their roles for supporting the system and using the principles of least privilege.  Access to the production environment is only allowed to members of specific security groups after approval. A subset of service team personnel has gone through the approval process for read-only access to production, used during critical incident escalations. Segregation of duties is established on critical functions within the Azure production environment, to minimize the risk of unauthorized changes to production services.  Access to make changes to the production environment is limited to authorized members in the service teams. Temporary elevated access to the production environment via JIT by other teams may be granted for specific issue handling or troubleshooting purposes.  To support segregation of duties and prevent unauthorized changes to production, Azure implements segregated environments. Development and testing responsibilities for new software builds or changes to existing software are segregated and managed through restricted access to branches within Azure DevOps and segregated development and test environments. Features and changes are developed by the service teams, reviewed by designated service team members and tested by the service team members for quality assurance and compatibility with the rest of the platform.  Azure maintains logical and physical separation between the development, test, and production environments. The development, test and production environments run on different clusters in separate network segments. Test and production clusters reside in separate network segments, which are accessed through distinct test and production Jumpboxes, Debug servers, and Network Hop Boxes. Access to test and production Jumpboxes, Debug servers, and Network Hop Boxes is restricted to authorized personnel.  Transfer of software to the production environment is controlled by a version control system (VCS). Deployment of software bits to production is controlled through approvals and on qualifying production entry criteria. Production deployments use approved software builds and images, and do not contain development tools and utilities. The test data resides in a segregated environment with access restricted to authorized individuals based on job responsibilities. Production data is not used for testing purposes in a way that affects customer service.  Physical access to servers and network devices is restricted to authorized personnel through the physical access protections in place at the datacenters. |

### CM-5(1) - Automated Access Enforcement and Audit Records

(a) Enforce access restrictions using [mechanisms used to automate the enforcement of access restrictions are defined;] ; and

(b) Automatically generate audit records of the enforcement actions.

|  |
| --- |
| **CM-5(1) Control Summary Information** |
| Responsible Roles: JIT, OneIdentity, Networking, Compute, Change Management |
| Parameter cm-05.01\_odp: organization-defined automated mechanisms |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CM-5(1) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for enforcing and auditing the access restrictions defined in CM-05.  **Azure**  **Servers and Services**  Service teams use Active Directory (AD) and JIT to control access to change functions. AD defines the access that is available, and JIT provides time-limited permission elevation when users need to use that access. AD and JIT are automated, and actions taken, including account creation, change, disabling, removal for AD and account elevation for JIT, are automatically audited.  **Network Devices**  Access restrictions are enforced via logical access security group restrictions. AD employs group membership, which requires security group owners to grant access to a given security group. AAA is integrated with a domain taxonomy of groups and users in AD. Both AD and AAA are supported via auditing mechanisms, which are captured via C+AI Security’s event collection environment. |

### CM-5(5) - Privilege Limitation for Production and Operation

(a) Limit privileges to change system components and system-related information within a production or operational environment; and

(b) Review and reevaluate privileges [at least quarterly].

|  |
| --- |
| **CM-5(5) Control Summary Information** |
| Responsible Roles: JIT, OneIdentity, Change Management |
| Parameter cm-5.5\_prm\_1: at least quarterly |
| Parameter cm-05.05\_odp.01: |
| Parameter cm-05.05\_odp.02: |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CM-5(5) What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for limiting privileges to make changes within customer-deployed production or operational environments.  **Azure**  Azure personnel do not have access to any of the Azure production environments to change hardware, software, or firmware components. Developers and integrators are responsible for developing the code, generating the builds, performing integration testing, and managing deployments. Azure limits privileges to release software and configuration changes to production to authorized personnel; only the designated approvers such as leads, managers, or PMs can approve changes to production, and the service teams deploy the changes using the DevOps model.  Segregation of duties is established on all critical functions within Azure’s production environment, to minimize the risk of unauthorized changes to productions services. As such, access to make changes to the production environment is limited to authorized service team members using the DevOps model.  Datacenter Services (DCS) Operations is responsible for managing physical access to the Azure environment. Physical access to the production environment is restricted to DCS personnel, who perform hardware changes. |
| **Part B**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for reviewing and reevaluating privileges defined in CM-05(05).a.  **Azure**  Azure service teams review access at least quarterly, consistent with normal account review processes. Access to servers and network devices is reviewed for appropriateness on a quarterly basis through review of access levels for physical access. |

## CM-6 Configuration Settings

a. Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using [common secure configurations to establish and document configuration settings for components employed within the system are defined;];

b. Implement the configuration settings;

c. Identify, document, and approve any deviations from established configuration settings for [system components for which approval of deviations is needed are defined;] based on [operational requirements necessitating approval of deviations are defined;] ; and

d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

(a) Requirement 1: The service provider shall use the DoD STIGs to establish configuration settings; Center for Internet Security up to Level 2 (CIS Level 2) guidelines shall be used if STIGs are not available; Custom baselines shall be used if CIS is not available.

(a) Requirement 2: The service provider shall ensure that checklists for configuration settings are Security Content Automation Protocol (SCAP) validated or SCAP compatible (if validated checklists are not available).

Guidance: Compliance checks are used to evaluate configuration settings and provide general insight into the overall effectiveness of configuration management activities. CSPs and 3PAOs typically combine compliance check findings into a single CM-6 finding, which is acceptable. However, for initial assessments, annual assessments, and significant change requests, FedRAMP requires a clear understanding, on a per-control basis, where risks exist. Therefore, 3PAOs must also analyze compliance check findings as part of the controls assessment. Where a direct mapping exists, the 3PAO must document additional findings per control in the corresponding SAR Risk Exposure Table (RET), which are then documented in the CSP's Plan of Action and Milestones (POA&M). This will likely result in the details of individual control findings overlapping with those in the combined CM-6 finding, which is acceptable. During monthly continuous monitoring, new findings from CSP compliance checks may be combined into a single CM-6 POA&M item. CSPs are not required to map the findings to specific controls because controls are only assessed during initial assessments, annual assessments, and significant change requests.

|  |
| --- |
| **CM-6 Control Summary Information** |
| Responsible Roles: Logging and Monitoring, Networking, SDL, Compute, Change Management |
| Parameter cm-06\_odp.01: Azure Security Benchmark |
| Parameter cm-06\_odp.02: all components |
| Parameter cm-06\_odp.03: approved operational requirements |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☒ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CM-6 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for establishing and documenting configuration settings for customer-deployed resources that reflect the most restrictive mode consistent with operational requirements.  **Azure**  **Servers and Secure Admin Workstations (SAWs)**  Microsoft establishes custom configuration baselines and configuration settings for its server assets. To establish these configuration settings, Microsoft examines and ingests a variety of sources:  \* Product architecture  \* Security analysis and principles, such as least functionality, least privilege, authorization and access control, auditing, network security, and operating system hardening  \* Microsoft Solution Accelerators Security Compliance Manager reference library  \* Vulnerability library knowledge bases  \* The United States Government Configuration Baseline USGCB  \* National Institute of Standards and Technology (NIST) recommendations  \* National Security Agency (NSA) recommendations  \* Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs)  \* Center for Internet Security (CIS) benchmarks  Microsoft works closely with CIS, DoD, NIST, and other regulators to establish the configuration settings and works with CIS as a participant during benchmark establishment. The configuration settings are primarily based on the CIS benchmarks and DISA STIGs, modified to address the unique operating environment of Azure. By evaluating and incorporating the best practices, guidance, and testing, Microsoft ensures a secure defense-in-depth deployment of technologies. The industry standards and input from baseline experts across Microsoft along with the environment-specific considerations and some role-specific settings (e.g. domain controller, workgroup server, domain joined server) are used to establish the configuration settings. The baseline for servers is published and made available to Microsoft personnel through the Azure DevOps source code repository, and a copy of the official baseline is published internally to the Liquid requirements catalog that is the authoritative source of requirements authored and maintained by Corporate, External and Legal Affairs (CELA) policy owners as well as other groups across Microsoft. The selected settings reflect the most restrictive, secure mode consistent with operational requirements. Microsoft ensures these settings can be scanned with traditional vulnerability scanners, enabling SCAP compliance on all applicable assets.  **Network Devices**  For network devices, Azure Networking defines the approved configuration baselines based on industry best practices and recommendations from the hardware manufacturers, taking into consideration any applicable criteria listed in the Azure details above. These configuration baselines are then established as Gold images from which all network devices are deployed and configured. Network devices are scanned by the vulnerability management tool, which meets SCAP requirements. |
| **Part B**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for implementing the configuration settings defined in CM-06.a.  **Azure**  **Servers and Secure Admin Workstations (SAWs)**  Mandatory configuration settings are implemented on each Azure asset as specified in the corresponding mandatory configuration baseline settings documentation for each component, which are established as described in Part a of this control. Azure service teams use Active Directory Group Policy Objects (GPOs) as an automated mechanism to centrally manage, apply, and verify security configuration settings. For virtual machines that are not domain-joined, Azure uses OS images that already have the appropriate settings configured prior to deployment.  **Network Devices**  Using the Gold images, Azure Networking configures all network devices with the required settings prior to deployment. Config Policy Verifier (CPV) compares the current network configuration against the configuration baseline and creates the proposed remediation for any deviations that are required. The results are reviewed and prioritized ongoing with major/critical items receiving priority remediation. |
| **Part C**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for identifying, documenting, and approving any deviations from established configuration settings for customer-deployed resources.  **Azure**  **Servers and Secure Admin Workstations (SAWs)**  There are currently no exceptions to the mandatory configuration settings in Azure, as all Azure components are running one of the approved builds. In the case of an exception, the exception is documented through the One Compliance System (1CS) exception process. If there is a need to deviate from the standard configuration settings, the Azure System Owner is required to approve the documented operational necessity for this deviation. All configuration changes are limited to the specific service team members responsible for the component and are captured as part of the workflow for the change management process defined in the Azure change process.  **Network Devices**  Exceptions may be discovered that requires temporary deviation from the mandatory configuration settings to avoid impacting production services while the issue is resolved. In these situations, Azure Networking takes the following actions:  \* The issue is triaged and discussed by Azure Networking Operations, and Azure Networking Engineering (including Azure Networking management) and a course of action is agreed upon and approved by this group.  \* The issue is discussed in the daily Azure Networking Operations meeting for general awareness.  \* The relevant policy in Config Policy Verifier (CPV) is temporarily altered.  \* The issue is fixed. As an example, this might involve deploying a new code revision to the affected devices.  \* The relevant policy in CPV is restored, and the configuration testing against the baseline resumes as usual.  **ACL Configuration Changes**  Security reviews are used by Azure and business groups to assess the security risks associated with non-standard operational implementations. Changes not expressly allowed by the Firewall and Tiered ACL guidelines (e.g. when an Azure team requests a non-standard change to configuration settings) are not allowed to be made to the Azure system’s current configuration without a completed review. Alternative to a quarterly review cycle, Azure performs these reviews real-time, prior to the implementation of the non-standard change (Configuration changes that are not automatically approved within the Firewall and Tiered ACL Guidelines).  To request a review, the requesting Azure team must populate a questionnaire, providing descriptions of the request, requirements, and justification for the change. Depending on the asset classification of data, descriptions may include data types, current compliance with data handling, and any risk assessment or threat analysis the Azure team has conducted in coordination with Privacy, CELA, or C+AI Security. The Azure team must also provide documentation to help the team that reviews (C+AI Security Solutions) assess operational risks (e.g. architecture and network diagrams, infrastructure threat models, etc.). |
| **Part D**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for monitoring and controlling changes to the configuration settings in accordance with organization policies and procedures.  **Azure**  **Servers and Secure Admin Workstations (SAWs)**  All configuration changes are limited to the specific personnel responsible for the component and are captured in audit logs. In addition, vulnerability scans are run to assist in determining the effectiveness of the configuration settings on the applications and servers.  Only certain individuals have the privileges to make changes to the configuration of the system based on an approved access model that requires establishing business justification for the membership. If an unauthorized person attempts to make changes, the system automatically denies the request. The action is captured in the audit logs and is investigated. If further actions are required, it is reported up to Azure and service team incident management personnel are notified immediately. The audit logs are maintained in storage for at least ninety (90) days to support after-the-fact investigations.  Installed software is monitored using Azure Security Monitoring (ASM) and SCUBA. If unauthorized software installation is detected, the Security Response Team responds.  **Network Devices**  Configuration baselines for network devices are incorporated as policies in Config Policy Verifier (CPV), which performs ongoing checks of all devices deployed on the network and reports deviations from standards. Upon discovering a deviation from the baseline, devices are corrected to ensure they agree with the current baseline. |

### CM-6(1) - Automated Management, Application, and Verification

Manage, apply, and verify configuration settings for [system components for which to manage, apply, and verify configuration settings are defined;] using [Assignment: organization-defined automated mechanisms].

|  |
| --- |
| **CM-6(1) Control Summary Information** |
| Responsible Roles: Logging and Monitoring, Networking, Compute, Change Management |
| Parameter cm-6.1\_prm\_2: All information system components |
| Parameter cm-06.01\_odp.01: organization-defined automated mechanisms |
| Parameter cm-06.01\_odp.02: |
| Parameter cm-06.01\_odp.03: |
| Parameter cm-06.01\_odp.04: |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CM-6(1) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for employing automated mechanisms to manage, apply, and verify configuration settings for customer-deployed resources.  **Azure**  Azure teams employ several tools to automatically manage, apply and verify configurations settings.  **Servers**  **IPAK**  The services running on Bare Metal and Pilotfish servers, including, but not limited to, Jumpboxes, Active Directory, Azure DNS, and other service teams, run standard Windows Server. The configuration baseline image for these assets is provided by the Imaging Production (IPAK) Engineering Team. The IPAK tool automates the installation of a standard set of applications, security fixes, and performance enhancements on Azure servers by providing a predictable and secure configuration in alignment with the Azure server baselines. Configuration baselines are developed by C+AI Security and then integrated into the IPAK for application to Azure servers. The IPAK is fully automatable or can be run manually, either locally on a single server, or remotely against many servers. The deployment of an IPAK includes the ability to access the summary log and preview status before and after an IPAK is deployed. IPAK logs are collected and can be previewed within the log collector tool, located on the IPAK site. This tool centrally manages and allows querying of log data for IPAK deployments.  **RDOS**  The RDOS team updates the server configuration baseline for Azure Host, Azure Native, and Azure Guest assets. The server base image is a version in which the kernel and many other core components have been modified to optimize them for the Azure environment. For service teams using Cloud Services, Windows server images are in the form of Virtual Hard Disks (VHDs) that are deployed as Guest VMs in the production environment. For Linux images, service teams use the Secure Base Image (SBI) that has been customized for secure configuration baselines relevant to Azure.  **Network Devices**  Config Policy Verifier (CPV) centrally monitors network device configurations, including verification of configuration settings and application and management of them. Device configuration settings are compared against network device baselines in the form of Gold images to determine consistency across the environment.  The Configuration Management process runs daily on all Azure network devices, verifying the device configuration against Azure Networking standard policies. The Summary report notes the number of failures and the number of devices tested. |

### CM-6(2) - Respond to Unauthorized Changes

Take the following actions in response to unauthorized changes to [configuration settings requiring action upon an unauthorized change are defined;]: [actions to be taken upon an unauthorized change are defined;].

|  |
| --- |
| **CM-6(2) Control Summary Information** |
| Responsible Roles: Logging and Monitoring, Incident Response, Networking, Compute, Change Management |
| Parameter cm-06.02\_odp.01: organization-defined configuration settings |
| Parameter cm-06.02\_odp.02: security-relevant configuration settings |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CM-6(2) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for employing security safeguards to respond to unauthorized changes to configuration settings for customer-deployed resources.  **Azure**  Azure Security has developed a set of auditable events specific to Azure. In the event of changes to security-relevant configuration settings, Azure Security invokes the incident management process.  In addition to auditable events, Azure utilizes Azure Security Monitoring (ASM) which is SCAP compatible to scan the environment for mandatory configuration changes. In the event of unauthorized changes to security-relevant configuration settings, Azure Security would invoke the incident management process. Each service team has a rotating list of members that are on call for response team efforts to investigate any unauthorized changes to security settings. |

## CM-7 Least Functionality

a. Configure the system to provide only [mission-essential capabilities for the system are defined;] ; and

b. Prohibit or restrict the use of the following functions, ports, protocols, software, and/or services: [Assignment: organization-defined prohibited or restricted functions, system ports, protocols, software, and/or services].

(b) Requirement: The service provider shall use Security guidelines (See CM-6) to establish list of prohibited or restricted functions, ports, protocols, and/or services or establishes its own list of prohibited or restricted functions, ports, protocols, and/or services if STIGs or CIS is not available.

|  |
| --- |
| **CM-7 Control Summary Information** |
| Responsible Roles: Logging and Monitoring, Networking, Compute, Change Management |
| Parameter cm-7(b): organization-defined mission essential capabilities |
| Parameter cm-07\_odp.01: functions, ports, protocols, and/or services identified as prohibited or restricted in the Azure Security Benchmark under Network Isolation (NetIso) |
| Parameter cm-07\_odp.02: |
| Parameter cm-07\_odp.03: |
| Parameter cm-07\_odp.04: |
| Parameter cm-07\_odp.05: |
| Parameter cm-07\_odp.06: |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CM-7 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for configuring customer-deployed resources to only provide essential capabilities (e.g., disabling extraneous services that may be provided by default, using a system for a single function rather than a system supporting multiple functions).  **Azure**  Azure takes into consideration the USGCB, DISA STIGs, CIS Benchmarks, vendor recommendations, and internal research in development of all operating system images, configuration scripts, and configuration files deployed within the system. These baselines help to ensure that only essential functions, ports, protocols, and services are enabled for each server. For network devices, the Azure Networking Standards and Architecture team sets the ACLs and configuration baseline standards for all network devices, using recommended configurations specific to each hardware vendor, and makes updates periodically based upon recommendations from the vendor. These configuration baselines help to ensure that only essential functions, ports, protocols, and services are enabled. |
| **Part B**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for prohibiting or restricting the use of specific functions, ports, protocols, and/or services to provide least functionality.  **Azure**  USGCB guidance, CIS Benchmarks, DISA STIGs, vendor recommendations, and internal research are taken into consideration during the development of operating system images. These images include essential functions, ports, protocols, and services. All other functions, ports, protocols, and services are disabled by default. The configuration baseline for ports and protocols allowed for Azure services are monitored by the C+AI Security team via Network Isolation (NetIso). C+AI Security monitors network configurations of Windows and Linux services for internet exposed management endpoints and high-risk ports and protocols as defined per the C+AI Platform security baseline process. Service teams must go through an approval process to have a port opened, or a function, protocol, or service enabled. For network devices, the Azure Networking Standards and Architecture team sets the configuration baseline standards for all network devices, using recommended configurations specific to each hardware vendor, and makes updates periodically based upon recommendations from the vendor. These configuration baselines include essential functions, ports, protocols, and services. |

### CM-7(1) - Periodic Review

(a) Review the system [at least annually] to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services; and

(b) Disable or remove [Assignment: organization-defined functions, ports, protocols, software, and services within the system deemed to be unnecessary and/or nonsecure].

|  |
| --- |
| **CM-7(1) Control Summary Information** |
| Responsible Roles: Logging and Monitoring, Networking, Compute, Change Management |
| Parameter cm-7.1\_prm\_2: any functions, ports, protocols, and services identified during the review process as unnecessary and/or non-secure |
| Parameter cm-07.01\_odp.01: at least monthly |
| Parameter cm-07.01\_odp.02: |
| Parameter cm-07.01\_odp.03: |
| Parameter cm-07.01\_odp.04: |
| Parameter cm-07.01\_odp.05: |
| Parameter cm-07.01\_odp.06: |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CM-7(1) What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for reviewing customer-deployed resources to identify unnecessary and/or unsecure functions, ports, protocols, and services.  **Azure**  Azure software and hardware configurations and Access Control Lists (ACLs) are reviewed at least monthly to identify any unnecessary or non-secure functions, ports, protocols, and services. |
| **Part B**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for disabling or removing functions, ports, protocols, software and services deemed to be unnecessary or unsecure.  **Azure**  Any function, port, protocol, software or service identified as unnecessary or non-secure during the review process is disabled. |

### CM-7(2) - Prevent Program Execution

Prevent program execution in accordance with [Selection (OneOrMore): [policies, rules of behavior, and/or access agreements regarding software program usage and restrictions are defined (if selected);] ;rules authorizing the terms and conditions of software program usage] .

Guidance: This control refers to software deployment by CSP personnel into the production environment. The control requires a policy that states conditions for deploying software. This control shall be implemented in a technical manner on the information system to only allow programs to run that adhere to the policy (i.e. allow-listing). This control is not to be based off of strictly written policy on what is allowed or not allowed to run.

|  |
| --- |
| **CM-7(2) Control Summary Information** |
| Responsible Roles: Logging and Monitoring, Networking, SDL, Change Management |
| Parameter cm-07.02\_odp.01: the SDL process |
| Parameter cm-07.02\_odp.02: |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☒ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CM-7(2) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for preventing program execution in accordance with customer-defined software program usage policies.  **Azure**  Installed software is monitored using Azure Security Monitoring (ASM) and SCUBA. If unauthorized software installation is detected, the Security Response Team responds.  Azure System Lockdown (AzSysLock) is a process in place to protect all Azure production assets from malicious code by ensuring only digitally signed and pre-authorized executables and scripts can run. Azure has implemented the capability needed to meet the requirement of preventing program execution. At this time, the ASM and SCUBA tools monitor assets for the software that has been installed but do not require preventing any unauthorized software from being installed. In the scenario of AzSysLock feature is turned off for Azure services, detections are sent to Azure service and security teams for activation actions. |

### CM-7(5) - Authorized Software - Allow-by-exception

(a) Identify [software programs authorized to execute on the system are defined;];

(b) Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system; and

(c) Review and update the list of authorized software programs [at least quarterly or when there is a change].

|  |
| --- |
| **CM-7(5) Control Summary Information** |
| Responsible Roles: Logging and Monitoring, Networking, Change Management |
| Parameter cm-07.05\_odp.01: software programs authorized to execute on the information system as defined in baselines and configuration scripts |
| Parameter cm-07.05\_odp.02: at least annually or when there is a change |
| Implementation Status (check all that apply):  ☐ Implemented  ☒ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CM-7(5) What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for identifying software programs authorized to execute on customer-deployed resources.  **Azure**  Azure identifies software authorized to execute within Azure via configuration baselines and configuration scripts. Both baselines and scripts are version controlled and under configuration management. Only software included in a baseline or configuration script may be installed on Azure. Azure uses Azure Security Monitoring (ASM) and SCUBA to identify unauthorized software execution and alert appropriate personnel for further review.  In addition to the standard release processes as part of OneBranch processes which includes build release verification steps such as virus scanning, in accordance with Microsoft Security Program Policy (MSPP), all software installed within Azure must have a valid signature. The Azure System Lockdown (AzSysLock) team uses AzSecPack to monitor for unexpected running software. This is defined as any software that is not signed using the appropriate signing certificates. AzSysLock sends alerts for service teams that are not properly using signed code. Additionally, for services running with AzSysLock in enforcement mode, which is currently an opt-in feature of AzSecPack, the binary does not run if it is not signed. Alerts for unsigned binaries running are created to service owners as a Severity 2 incident. In the scenario of AzSysLock feature is turned off for Azure services, detections are sent to Azure service and security teams for activation actions.  For services running Azure Security Pack (AzSecPack), the OS security configuration baseline is also monitored for baseline violations, which are then reported to service owners through Incident Management (IcM) and/or Service 360 (S360) depending on the severity of the violation. Near real-time alerts include alerts for audit processing failures, such as system time changes or audit policy changes.  Additionally, virtual components within Azure are managed by the Fabric Controller (FC), which is the component that is used to create, monitor, restart, and destroy virtual machines. Overall VM and Azure Host/Native management coverage of AzSecPack is maintained by AzSecPack. |
| **Part B**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for employing a deny-all, permit-by-exception policy to allow the execution of authorized software programs on customer-deployed resources.  **Azure**  Azure employs a deny-by-default, permit-by-exception software policy. Any changes to baselines or configuration scripts must be reviewed and approved by the appropriate change review committee. |
| **Part C**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for reviewing and updating the list of authorized software programs.  **Azure**  Azure service teams review and update baselines and configuration scripts at least annually. |

## CM-8 System Component Inventory

a. Develop and document an inventory of system components that:

1. Accurately reflects the system;

2. Includes all components within the system;

3. Does not include duplicate accounting of components or components assigned to any other system;

4. Is at the level of granularity deemed necessary for tracking and reporting; and

5. Includes the following information to achieve system component accountability: [information deemed necessary to achieve effective system component accountability is defined;] ; and

b. Review and update the system component inventory [at least monthly].

Requirement: must be provided at least monthly or when there is a change.

|  |
| --- |
| **CM-8 Control Summary Information** |
| Responsible Roles: Networking, Asset Management, Datacenter Hosting |
| Parameter cm-08\_odp.01: unique asset identifier, hardware type, NetBIOS name, baseline configuration name, OS name, IP address, host name, server name, property group, serial number, Microsoft asset number, datacenter, collocation, location zone, rack, rack slot number, environment, manufacturer, model, and function |
| Parameter cm-08\_odp.02: at least monthly |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CM-8 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for developing and documenting an inventory of customer-deployed resources, that supports tracking and reporting, and includes any information the customer has deemed necessary to achieve effective accountability.  **Azure**  After collecting inventory information from the below sources and teams, Azure consolidates the information and performs month-over-month data analysis and reconciliation. Any changes to, additions to, or removals from the inventory are identified, verified, and explained. This data is stored within the Kusto, EventHub, and Cosmos tools. For all asset types, the inventory is consistent with the authorization boundary because it is kept up to date with new installations and decommissioning of devices.  The inventory of logical assets are tracked in service Privacy Review documentation, which is reviewed as a part of the regular privacy review, or when there is a new component being reviewed as a part of the new feature Privacy Review. The Privacy Review documentation also maintains the retention requirements of the data as per regulatory requirements.  The inventory of all assets for Azure services must be maintained by and are obtained from the service owners using the following methods.The management of inventory by service owners ensures there is no duplicate accounting of inventory and assets are assigned a unique identifier.  **Servers**  Physical inventory data is pulled daily from nine different sources, both available to customers and internal tools. These sources include OneAsset, Cedis, GDCO App, ImageOps, Rescue\_DNS, DCM, MSODS, DERA, AzSecSlam, DCMT, Cockpit, VMAC, Intune, Active Directory (AD), DNS, Network Graph Service (NGS), and Fabric2. These sources are maintained by each individual service team.  **Host**  The Host inventory consists of nodes which have VM containers running on top of them. Nodes are differentiated by the type of work they do. If a node hosts virtual machines, then it is a Host node. If a node doesn't have virtual machines and the entire node is in use, then it is a Native node. Host inventory data is generated automatically using subscription data.  **Native**  Native data is generated automatically using subscription data.  **Infraguest**  Infraguest data is generated from subscriptions within Service Tree and the SQL team. Those subscriptions are then used to query Geneva Actions; each service team owns Azure subscriptions, and Geneva Actions generates reports showing all of the virtual machines belonging to each subscription ID.  **Bare Metal**  The Bare Metal server inventory is defined as assets that are not managed by either Azure or Auto Pilot/Pilot Fish. The asset type Includes both physical servers and virtual machines. The inventory mapping is done through Service Tree. All Global Datacenter Operations (GDCO) app assets are assigned a Property Group and Property Dimension. These are assigned the ownership. Service Tree takes the owner associated and assigns a service based on the owner’s division.  **Pilotfish**  Pilotfish data is generated from the Pilotfish team, which provides a Kusto cluster database that the Inventory team ingests to get the data.  **Network Devices**  Network data is populated from streams from the Azure Networking team. The Azure Networking team provides device data in Kusto which is processed by the Inventory team to add other attributes like Service Tree Name and asset identifier.  **Services**  Asset information includes the responsible Azure service team. This ensures that no other information system identifies an asset as part of that information system. Service ownership is always at the  asset level and Azure has various methods of determining ownership. Service teams own and manage Azure subscriptions which they use to deploy virtual machines and other services. Each subscription has a corresponding subscription ID. Property Dimension and Property Group mappings are used for Bare Metal machines which correlate to Service Tree ownership. This helps to ensure Microsoft only ever has a 1-to-1 mapping between assets and a service.  **Databases**  Database information is calculated based upon the inventory of physical and virtual servers received from each team. |
| **Part B**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for reviewing and updating the inventory defined in CM-08.a.  **Azure**  Azure Fleet Inventory ingests the asset type sources providing the asset data every couple of hours and source teams provide data anywhere from every hour to every 24 hours. Azure updates the system inventory at least monthly using the sources identified and includes updated inventory information in the monthly Continuous Monitoring report provided to the authorizing officials. |

### CM-8(1) - Updates During Installation and Removal

Update the inventory of system components as part of component installations, removals, and system updates.

|  |
| --- |
| **CM-8(1) Control Summary Information** |
| Responsible Roles: Networking, Asset Management, Datacenter Hosting |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CM-8(1) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for reviewing and updating the inventory of customer-deployed resources when installations, removals, and system updates occur.  **Azure**  Azure service teams are responsible for updating the inventory of information system components using Service Tree, Property Groups, and Property Dimensions as an integral part of component installations, removals, and information system updates. The inventory tracks specific inventory information for all Azure assets. Additionally, Azure generates a complete inventory each month, and analyzes and reconciles all changes from the previous month’s inventory.  As an additional protection, Azure employs strict physical access controls in the datacenters to mitigate the unauthorized addition of new devices into the environment. Physical access to the devices to add additional ports is also disabled within the environment. |

### CM-8(2) - Automated Maintenance

Maintain the currency, completeness, accuracy, and availability of the inventory of system components using [Assignment: organization-defined automated mechanisms].

|  |
| --- |
| **CM-8(2) Control Summary Information** |
| Responsible Roles: Networking, Asset Management, Datacenter Hosting |
| Parameter cm-8.2\_prm\_1: organization-defined automated mechanisms |
| Parameter cm-08.02\_odp.01: |
| Parameter cm-08.02\_odp.02: |
| Parameter cm-08.02\_odp.03: |
| Parameter cm-08.02\_odp.04: |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CM-8(2) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for employing automated mechanisms to maintain an up-to-date, complete, accurate, and readily available inventory of customer-deployed resources.  **Azure**  Azure uses numerous automated mechanisms for ensuring the inventory is accurate, including Service Tree for subscriptions and team mappings, Geneva Actions, and GDCO App. |

### CM-8(3) - Automated Unauthorized Component Detection

(a) Detect the presence of unauthorized hardware, software, and firmware components within the system using [automated mechanisms with a maximum five-minute delay in detection] [continuously] ; and

(b) Take the following actions when unauthorized components are detected: [Selection (OneOrMore): disable network access by unauthorized components;isolate unauthorized components;notify [personnel or roles to be notified when unauthorized components are detected is/are defined (if selected);] ] .

|  |
| --- |
| **CM-8(3) Control Summary Information** |
| Responsible Roles: Logging and Monitoring, Incident Response, Networking, Asset Management, Datacenter Hosting, Change Management |
| Parameter cm-8.3\_prm\_1: isolates the components by default |
| Parameter cm-08.03\_odp.01: |
| Parameter cm-08.03\_odp.02: |
| Parameter cm-08.03\_odp.03: |
| Parameter cm-08.03\_odp.04: disables network access by such components |
| Parameter cm-08.03\_odp.05: service team administrators, Security Incident Response (SIR) team |
| Parameter cm-08.03\_odp.06: |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CM-8(3) What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for employing automated mechanisms to detect the presence of unauthorized software within customer-deployed resources and take action when unauthorized components are detected.  **Azure**  As a primary protection, Azure employs strict physical access controls in the datacenters to mitigate the unauthorized addition of new devices into the environment. Physical access to the devices to add additional ports is also disabled within the environment.  **Servers**  In addition to the standard release processes as part of OneBranch processes which includes build release verification steps such as virus scanning, in accordance with Microsoft Security Program Policy (MSPP), all software installed within Azure must have a valid signature. The Azure System Lockdown (AzSysLock) team uses AzSecPack to monitor for unexpected running software. This is defined as any software that is not signed using the appropriate signing certificates. AzSysLock sends alerts for service teams that are not using signed code. Additionally, for services running with AzSysLock in enforcement mode, which is currently an opt-in feature of AzSecPack, the binary does not run if it is not signed. Alerts for unsigned binaries running are created to service owners as a Severity 2 incident. In the scenario of AzSysLock feature is turned off for Azure services, detections are sent to Azure service and security teams for activation actions.  AzSecPack also monitors the server security configuration baseline for baseline violations, which are then reported to service owners through Incident Management (IcM) and/or Service 360 (S360) depending on the severity of the violation. Near real-time alerts include alerts for audit processing failures, such as system time changes or audit policy changes.  Additionally, virtual components within Azure are managed by the Fabric Controller (FC), which is the component that is used to create, monitor, restart, and destroy virtual machines. Overall VM and Azure Host/Native management coverage of AzSecPack is maintained by AzSecPack.  **Network Devices**  All network devices managed by Azure Networking go through the Configuration Policy Verifier (CPV) tool. This tool is executed on all devices which are in buildout to run a series of acceptance tests on devices before they are marked ready for production. |
| **Part B**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for taking action when unauthorized software is detected.  **Azure**  Azure Security monitors services using the Geneva Monitoring Agent (MA). The MA aggregates monitoring information for review. When relevant events are detected, such as the unauthorized installation of software, it generates an alert to the appropriate personnel for triage and response. |

### CM-8(4) - Accountability Information

Include in the system component inventory information, a means for identifying by [Selection (OneOrMore): name;position;role] , individuals responsible and accountable for administering those components.

|  |
| --- |
| **CM-8(4) Control Summary Information** |
| Responsible Roles: Asset Management, Datacenter Hosting |
| Parameter cm-08.04\_odp: service team |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CM-8(4) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for including the individual(s) responsible/accountable for administering the customer-deployed resources listed in the inventory (see CM-08.a).  **Azure**  Inventory information includes the service team responsible for each component within Azure. Each service team designates one or more individuals or roles responsible for administering that team’s components. These individuals can also be identified by position and role as necessary, and are present in Service Tree. |

## CM-9 Configuration Management Plan

Develop, document, and implement a configuration management plan for the system that:

a. Addresses roles, responsibilities, and configuration management processes and procedures;

b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;

c. Defines the configuration items for the system and places the configuration items under configuration management;

d. Is reviewed and approved by [personnel or roles to review and approve the configuration management plan is/are defined;] ; and

e. Protects the configuration management plan from unauthorized disclosure and modification.

Guidance: FedRAMP does not provide a template for the Configuration Management Plan. However, NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems, provides guidelines for the implementation of CM controls as well as a sample CMP outline in Appendix D of the Guide

|  |
| --- |
| **CM-9 Control Summary Information** |
| Responsible Roles: SOP Team, SDL |
| Parameter cm-9(d): the Azure SOP Review Process Authority |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CM-9 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for developing, documenting, and implementing a configuration management plan that addresses roles, responsibilities, and configuration management processes and procedures.  **Azure**  Azure has system-wide configuration management requirements and processes documented in its Azure Standard Operating Procedures (SOPs). These documents contain high-level roles and responsibilities, defines configuration management processes, and identifies configuration items as well as procedures for maintaining configuration items. All Azure service teams are required to comply with all SOPs, which are maintained appropriately.  \* Azure Security Baseline Governance Standard Operating Procedure (SOP)  \* Azure Security Development Lifecycle Standard Operating Procedure (SOP)  \* Azure Hardware Change and Release Management Standard Operating Procedure (SOP)  \* Azure Software Change and Release Management Standard Operating Procedure (SOP) |
| **Part B**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for developing, documenting, and implementing a configuration management plan that establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of customer-deployed resources.  **Azure**  The Azure SOPs define configuration items at the hardware and software levels. |
| **Part C**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for developing, documenting, and implementing a configuration management plan that defines the configuration items for the customer-deployed resources and places the configuration items under configuration management.  **Azure**  Azure defines the configuration items for the information system. Azure aligns with Microsoft’s Security Development Lifecycle (SDL) process which documents each phase of development that must be followed for all engineering projects. The Azure SOPs cover the change management process around information system design, development, and implementation of changes. When a component of Azure is initiated using the SDL process, it is placed under the Microsoft and Azure configuration management requirements. |
| **Part D**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for reviewing and approving the configuration management plan.  **Azure**  The Azure SOP Review Process Authority reviews and approves Azure SOPs on an annual basis. |
| **Part E**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for developing, documenting, and implementing a configuration management plan that protects the configuration management plan from unauthorized disclosure and modification.  **Azure**  The Azure SOPs are stored within the Azure SharePoint site, which has functionality enable to protect against unauthorized disclosure and modification. |

## CM-10 Software Usage Restrictions

a. Use software and associated documentation in accordance with contract agreements and copyright laws;

b. Track the use of software and associated documentation protected by quantity licenses to control copying and distribution; and

c. Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

|  |
| --- |
| **CM-10 Control Summary Information** |
| Responsible Roles: Compute, Change Management, CELA |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CM-10 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for using software and associated documentation in accordance with contract agreements and copyright laws.  **Azure**  The Microsoft Acceptable Use Standard outlines the Online Services specific acceptable usage standards of the Infrastructure & Services technology assets, including criteria including whether roles can make copies of copyrighted software. The Copyright Policy also contains information on how Microsoft respects copyright law.  In accordance with the Third Party Software Policy, Azure uses software according to contractual agreements. This portion of the corporate policy states the following: Unlike other types of finished goods, software is not owned by end users, but licensed through a contractual agreement which defines the terms and conditions that govern the license grant and restrict the product’s use. These terms and conditions may change over time through amendment, renewal, termination, expiration, etc. |
| **Part B**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for tracking the use of software and associated documentation protected by quantity licenses.  **Azure**  The Microsoft Security Policy (MSP) outlines the software usage restrictions for Azure and requires all Azure applications, including those developed or hosted by and/or purchased from third parties, to undergo a comprehensive security review before entry into the Azure environment. In addition, no software is to be deployed or used in Azure’s production environment without formal approval as required by the MSP.  In-house software used within the Azure boundary is developed by Microsoft and, therefore, not subject to contractual requirements, copyright restrictions, and licenses monitoring for compliance with third-party relationships.  In accordance with the Third Party Software Policy, all third-party software must be purchased through a corporate function to enable tracking of all software purchases, compliance with software licensing terms, and corporate risk reduction from exposure to licensing agreements. Microsoft complies with all software usage requirements as defined by the contractual agreement with the vendor. |
| **Part C**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for controlling and documenting of the use of peer-to-peer (P2P) file sharing technology to prevent unauthorized distribution, display, performance, or reproduction of copyrighted work.  **Azure**  Azure configures the information system to provide only essential capabilities and specifically prohibits or restricts the use of functions, ports, protocols, and/or services as per industry best practice guidelines. Any use of peer-to-peer (P2P) networking in the environment is denied by default. If needed, P2P networking would be managed as an exception through the security review process. Furthermore, Azure prohibits the distribution of pirated software in accordance with Microsoft Policy. |

## CM-11 User-installed Software

a. Establish [policies governing the installation of software by users are defined;] governing the installation of software by users;

b. Enforce software installation policies through the following methods: [methods used to enforce software installation policies are defined;] ; and

c. Monitor policy compliance [Continuously (via CM-7 (5))].

|  |
| --- |
| **CM-11 Control Summary Information** |
| Responsible Roles: Logging and Monitoring, Change Management, CELA |
| Parameter cm-11\_odp.01: Microsoft policy |
| Parameter cm-11\_odp.02: configuration control processes described in CM-03 and access restrictions for change described in CM-05 |
| Parameter cm-11\_odp.03: continuously (via CM-07(05)) |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CM-11 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for establishing a policy governing the installation of software on customer-deployed resources by users.  **Azure**  The Microsoft Security Policy (MSP) outlines the Microsoft user-installed software restrictions for Azure. In accordance with the policy, all software installed in the Azure environment, prior to being released into production, must go through the change management process and be approved by the appropriate stakeholders. The following guidelines are in place regarding the installation of software, including open source software, within the Azure environment:  \* All software installed within Azure must be approved by the appropriate stakeholders prior to being released into production.  \* Prior to deployment in Azure, all software must be tested in a manner suitable to Microsoft to evaluate its impact on system performance, stability (failure and recovery characteristics) and security state (security controls work as expected and the product does not contain malicious code).  \* Software submitted for approval must have a legitimate business purpose.  Additionally, open source software must be evaluated by Corporate, External and Legal Affairs (CELA) in accordance with the policies and processes set out in Microsoft’s open source software resource website. Requests for evaluation of open source software require approval through the OSS Registration Tool. |
| **Part B**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for enforcing software installation policies.  **Azure**  Azure enforces software installation policies through configuration control processes and access restrictions for change. |
| **Part C**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for monitoring the compliance of customer-deployed resources with the policies identified in CM-11.a.  **Azure**  Azure monitors compliance by reviewing and updating configuration settings and configuration baselines of hardware, software and network devices at least annually. Changes are developed, tested and approved prior to entering the production environment in a development and/or test environment. |

## CM-12 Information Location

a. Identify and document the location of [information for which the location is to be identified and documented is defined;] and the specific system components on which the information is processed and stored;

b. Identify and document the users who have access to the system and system components where the information is processed and stored; and

c. Document changes to the location (i.e., system or system components) where the information is processed and stored.

Requirement: According to FedRAMP Authorization Boundary Guidance

|  |
| --- |
| **CM-12 Control Summary Information** |
| Responsible Roles: JIT, OneIdentity, SDL, Asset Management, Datacenter Hosting, Change Management, Supply Chain |
| Parameter cm-12(a): organization-defined information |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CM-12 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  The customer is responsible for identifying and documenting the location of system inventory components for customer-deployed resources.  **Azure**  Information system components that make up Azure cloud environments consist of physical digital media hardware and logical software. Both digital media and logical software components of Azure cloud environments are housed in Azure datacenters deployed in United States geographic locations. The physical address locations of Azure datacenters are documented in facility manager tool utilized by datacenter personnel. |
| **Part B**  **Customer Responsibility**  The customer is responsible for building out appropriate access control procedures for managing personnel who have access to the inventory system components for customer-deployed resources.  **Azure**  Information system components that make up Azure cloud environments consist of physical digital media hardware and logical software. Both digital media and logical software components of Azure cloud environments are housed in Azure datacenters deployed in United States geographic locations.  Physical access to digital media in Azure datacenters is managed by Datacenter Access Tool (DCAT). DCAT contains the authorized access lists of personnel who have been approved by the Datacenter Management (DCM) team. Access to areas within the datacenter is granted based on the least privileged principle. Before a person arrives at a data center, they must have a DCAT request approved by the DCM team.  For logical software, privileges to Azure production services and administrative interfaces are assigned to Azure personnel based on the least privilege principles in accordance with job responsibilities. Elevated access must be approved by the respective account managers. OneIdentity aliases, used for access provisioning to resources, are based on structured business resources/rules created by the Azure service teams. They are used to grant Azure personnel access to designated and restricted security groups on least privilege principles. Service teams can obtain Just in Time (JIT) for troubleshooting purposes. JIT is utilized to limit elevated access to a specific duration of time, eliminating the use of persistent elevated access. JIT access is provided though the JIT portal based on the workflow configured and the access is granted only to the requested assets. The access can be configured to support business needs and can range from one (1) hour to seven (24) hours and revoked based on the JIT policy settings prescribed by the resource owner. Break-Glass accounts provide the minimum permissions necessary to execute work if JIT is nonfunctioning. Access to Azure services is granted based upon need-to-know and least privileged principles. Access that has not been explicitly permitted is denied by default. Role-based access controls are used to allocate logical access to a specific job function or area of responsibility, rather than to an individual. |
| **Part C**  **Customer Responsibility**  The customer is responsible for managing changes relating to the location of the system inventory components for customer-deployed resources.  **Azure**  Information system components that make up Azure cloud environments consist of physical digital media hardware and logical software. Both digital media and logical software components of Azure cloud environments are housed in Azure datacenters deployed in United States geographic locations. The physical address locations of Azure datacenters are documented in facility manager tool utilized by datacenter personnel. If changes to the location of the Azure datacenters occur within the United States geographic country, data center personnel will document the occurrence in facility manager tool. |

### CM-12(1) - Automated Tools to Support Information Location

Use automated tools to identify [Federal data and system data that must be protected at the High or Moderate impact levels] on [system components where the information is located are defined;] to ensure controls are in place to protect organizational information and individual privacy.

Requirement: According to FedRAMP Authorization Boundary Guidance.

|  |
| --- |
| **CM-12(1) Control Summary Information** |
| Responsible Roles: JIT, OneIdentity, SDL, Asset Management, Datacenter Hosting, Change Management, Supply Chain |
| Parameter cm-12.01\_odp.01: organization-defined information by information type |
| Parameter cm-12.01\_odp.02: organization-defined system components |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CM-12(1) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for utilizing automated tools to identify customer-controlled information system components to ensure controls are in place to protect customer information.  **Azure**  Information system components that make up Azure cloud environments consist of physical digital media hardware and logical software. Both digital media and logical software components of Azure cloud environments are housed in Azure datacenters deployed in United States geographic locations. The physical address locations of Azure datacenters are documented in facility manager tool utilized by datacenter personnel.  Physical access to digital media in Azure datacenters is managed by Datacenter Access Tool (DCAT). DCAT contains the authorized access lists of personnel who have been approved by the Datacenter Management (DCM) team. Access to areas within the datacenter is granted based on the least privileged principle. Before a person arrives at a data center, they must have a DCAT request approved by the DCM team. For logical software, privileges to Azure production services and administrative interfaces are assigned to Azure personnel based on the least privilege principles in accordance with job responsibilities. Elevated access must be approved by the respective account managers. OneIdentity aliases, used for access provisioning to resources, are based on structured business resources/rules created by the Azure service teams. They are used to grant Azure personnel access to designated and restricted security groups on least privilege principles. Service teams can obtain Just in Time (JIT) for troubleshooting purposes. JIT is utilized to limit elevated access to a specific duration of time, eliminating the use of persistent elevated access. JIT access is provided though the JIT portal based on the workflow configured and the access is granted only to the requested assets. The access can be configured to support business needs and can range from one (1) hour to seven (24) hours and revoked based on the JIT policy settings prescribed by the resource owner. Break-Glass accounts provide the minimum permissions necessary to execute work if JIT is nonfunctioning. Access to Azure services is granted based upon need-to-know and least privileged principles. Access that has not been explicitly permitted is denied by default. Role-based access controls are used to allocate logical access to a specific job function or area of responsibility, rather than to an individual.  If changes to the location of the Azure datacenters occur within the United States geographic country, data center personnel will document the occurrence in facility manager tool. |

## CM-14 Signed Components

Prevent the installation of [Assignment: organization-defined software and firmware components] without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.

Guidance: If digital signatures/certificates are unavailable, alternative cryptographic integrity checks (hashes, self-signed certs, etc.) can be utilized.

|  |
| --- |
| **CM-14 Control Summary Information** |
| Responsible Roles: Logging and Monitoring, Incident Response, Networking, SDL, Asset Management, Datacenter Hosting, Change Management, Supply Chain |
| Parameter cm-14: all software and firmware components |
| Parameter cm-14\_odp.01: |
| Parameter cm-14\_odp.02: |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CM-14 What is the solution and how is it implemented?** |
| **Customer Responsibility**  For IaaS and PaaS assets, the customer is responsible for prevent the installation of organization-defined software and firmware components without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.  **Azure**  In accordance with Microsoft Security Program Policy (MSPP), all software installed within Azure must have a valid signature. The Azure System Lockdown (AzSysLock) team uses AzSecPack to monitor for unexpected running software. This is defined as any software that is not signed using the appropriate signing certificates. AzSysLock sends alerts for service teams that are not using signed code. Additionally, for services running with AzSysLock in enforcement mode, which is currently an opt-in feature of AzSecPack, the binary does not run if it is not signed. Alerts for unsigned binaries running are created to service owners as a Severity 2 incident in the Incident Management (IcM) system. In the scenario of AzSysLock feature is turned off for Azure services, detections are sent to Azure service and security teams for activation actions. |

# Contingency Planning (CP)

## CP-1 Policy and Procedures

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (OneOrMore): organization-level;mission/business process-level;system-level] contingency planning policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the contingency planning policy and the associated contingency planning controls;

b. Designate an [an official to manage the contingency planning policy and procedures is defined;] to manage the development, documentation, and dissemination of the contingency planning policy and procedures; and

c. Review and update the current contingency planning:

1. Policy [at least annually] and following [events that would require the current contingency planning policy to be reviewed and updated are defined;] ; and

2. Procedures [at least annually] and following [significant changes].

|  |
| --- |
| **CP-1 Control Summary Information** |
| Responsible Roles: SOP Team, Policy |
| Parameter cp-1(a): all personnel |
| Parameter cp-01\_odp.01: |
| Parameter cp-01\_odp.02: |
| Parameter cp-01\_odp.03: a Microsoft-wide |
| Parameter cp-01\_odp.04: the Microsoft Information Risk Management Council (IRMC) organization |
| Parameter cp-01\_odp.05: at least annually |
| Parameter cp-01\_odp.06: significant changes |
| Parameter cp-01\_odp.07: at least annually |
| Parameter cp-01\_odp.08: significant changes |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☒ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CP-1 What is the solution and how is it implemented?** |
| **Part A1**  **Customer Responsibility**  The customer is responsible for developing, documenting, and disseminating contingency planning policy and procedures that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.  **Azure**  Azure addresses the contingency planning policy as part of the Microsoft security policies, of which there are two sets: the Microsoft Security Policy (MSP) that is applicable to all Microsoft personnel, and the Microsoft Security Program Policy (MSPP), which is applicable to all Microsoft personnel that have a responsibility for security. The Microsoft Information Risk Management Council (IRMC) is the governance body with review and approval responsibility for the MSP and MSPP. Within Azure, the MSPP specifically applies to all Microsoft personnel with security objectives such as designing, building, and operating Azure and across all information and processes used in the conduct of Microsoft business. All Azure personnel are accountable and responsible for complying with these guiding principles within their designated roles. The policy addresses the following:  \* Business continuity process  \* Alternate systems facilities  \* Service resiliency  Additionally, the policy addresses the purpose, scope, roles, responsibilities, compliance requirements, and required coordination among the various Microsoft organizations that provide some level of support to all services. The standards indicate Microsoft management’s commitment and are a component of the risk management strategy which provides Azure personnel with a current set of clear and concise information security requirements.  The MSP is available to all Microsoft personnel on the Microsoft Policy website on the Microsoft intranet, and the MSPP and Security Standards are available through the Liquid tool, also on the Microsoft intranet. The Azure SOPs are stored in the Azure Security, Privacy & Compliance SharePoint site. This SharePoint site is accessible to all Azure personnel.  The Azure BCM System Manual is maintained in the Azure Business Continuity and Disaster Recovery (BCDR) website on the Microsoft intranet.  Service teams may supplement the Azure policies and procedures with offering-specific policies and procedures. Service-team-specific policies and procedures associated with contingency planning are documented and stored within internal Azure SharePoint sites. Only personnel with authorized credentials, adequate levels of permission, legitimate need to know, and specific roles and responsibilities are given access to the service-team-specific policies or procedures. |
| **Part A2**  **Customer Responsibility**  The customer is responsible for procedures to facilitate the implementation of the contingency planning policy and the associated configuration management controls.  **Azure**  The Azure Business Continuity and Disaster Recovery Standard Operating Procedure (SOP) implements the contingency planning policy and associated controls. Azure also implements policy and procedures through the Business Continuity Management (BCM) System Manual managed by the C+AI Azure Business Continuity Management team. The purpose of this manual is to document the BCM methods and approach to be implemented by Azure services, internal Azure groups, and support functions. It defines the purpose of the program and sets forth the drivers, goals, objectives, and strategies that are used as guiding principles. The BCM program is in alignment with those of Microsoft’s Enterprise Business Continuity Management (EBCM) Program. The SOP and BCM System Manual document the following procedures:  \* Continuity management process  \* Business impact and dependency analysis  \* Writing and implementing continuity plans  \* Continuity planning framework  Service teams may supplement the Azure policies and procedures with offering-specific policies and procedures. Service-team-specific policies and procedures associated with contingency planning are documented and stored within internal Azure SharePoint sites. Only personnel with authorized credentials, adequate levels of permission, legitimate need to know, and specific roles and responsibilities are given access to the service-team-specific policies or procedures. |
| **Part B**  **Customer Responsibility**  The customer is responsible for designating an official to manage the development, documentation, and dissemination of the contingency planning policy and procedures.  **Azure**  The Microsoft Information Risk Management Council (IRMC) organization is the governance body with approval responsibility for the Microsoft Security Policy (MSP) and Microsoft Security Program Policy (MSPP). The IRMC consists of representatives from security and risk management teams across Microsoft including Core Services Engineering and Operations (CSEO), Azure, and Global Security. The Customer Security and Trust: Security Engineering (CST-SE) organization manages the review and approval process and maintains the policies.  On an annual basis, the CST-SE conducts a line-by-line review of the MSP and MSPP. The Microsoft Security Policy (MSP) and Microsoft Security Program Policy (MSPP) Governance document describes each member’s role, types and frequency of review, escalation paths, approval process, and formal publishing procedures of the security policy. Throughout the year, if necessary, CST-SE may convene with the IRMC to conduct reviews after a significant review or change request. The approved policy update is published within the relevant tool on the Microsoft intranet. If service teams establish service-specific or team-specific policies, the respective service teams update the necessary policies at least annually. |
| **Part C1**  **Customer Responsibility**  The customer is responsible for reviewing and updating the current contingency planning policy on a regular basis and following organization defined events.  **Azure**  The Azure team updates the Azure SOPs at least annually through a formal review process. If needed, the Azure team updates the SOP after a significant change affecting policy execution as well. If established, service-team-specific procedures are updated by their respective teams. The individual service teams review and update their respective SOPs at least annually and when required by a significant change. |
| **Part C2**  **Customer Responsibility**  The customer is responsible for reviewing and updating the current contingency planning procedures on a regular basis and following organization defined events.  **Azure**  The Azure team updates the Azure SOPs at least annually through a formal review process. If needed, the Azure team updates the SOP after a significant change affecting policy execution as well. If established, service-team-specific procedures are updated by their respective teams. The individual service teams review and update their respective SOPs at least annually and when required by a significant change. |

## CP-2 Contingency Plan

a. Develop a contingency plan for the system that:

1. Identifies essential mission and business functions and associated contingency requirements;

2. Provides recovery objectives, restoration priorities, and metrics;

3. Addresses contingency roles, responsibilities, assigned individuals with contact information;

4. Addresses maintaining essential mission and business functions despite a system disruption, compromise, or failure;

5. Addresses eventual, full system restoration without deterioration of the controls originally planned and implemented;

6. Addresses the sharing of contingency information; and

7. Is reviewed and approved by [Assignment: organization-defined personnel or roles];

b. Distribute copies of the contingency plan to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements];

c. Coordinate contingency planning activities with incident handling activities;

d. Review the contingency plan for the system [at least annually];

e. Update the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;

f. Communicate contingency plan changes to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements];

g. Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training; and

h. Protect the contingency plan from unauthorized disclosure and modification.

Requirement: For JAB authorizations the contingency lists include designated FedRAMP personnel.

Requirement: CSPs must use the FedRAMP Information System Contingency Plan (ISCP) Template (available on the fedramp.gov: https://www.fedramp.gov/assets/resources/templates/SSP-A06-FedRAMP-ISCP-Template.docx).

|  |
| --- |
| **CP-2 Control Summary Information** |
| Responsible Roles: BCDR |
| Parameter cp-2(a)(7): Azure Information System Security Officer |
| Parameter cp-2(b): Azure Incident Management Team (AIM) and FedRAMP personnel specified by the JAB |
| Parameter cp-2(f): Azure Incident Management Team (AIM) and FedRAMP personnel specified by the JAB |
| Parameter cp-02\_odp.01: |
| Parameter cp-02\_odp.02: |
| Parameter cp-02\_odp.03: |
| Parameter cp-02\_odp.04: |
| Parameter cp-02\_odp.05: at least annually |
| Parameter cp-02\_odp.06: |
| Parameter cp-02\_odp.07: |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CP-2 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for developing a contingency plan for customer-deployed resources, including essential mission and business functions and associated contingency requirements; recovery objectives, restoration priorities and metrics; contact information for assigned roles/responsibilities/individuals; maintaining essential mission and business functions despite system disruption, compromise or failure; eventual, full system restoration without deterioration of originally implemented security safeguards; and review/approval of the plan by customer-defined personnel/roles. Note: the customer should also include any reliance on Azure functionality to perform these tasks.  **Azure**  The Azure Business Continuity Plan (BCP) and Azure Disaster Recovery Plan (DRP) provide the detailed processes for contingency planning for Azure. They serve as a guide for Azure to respond, recover, and resume operations during a serious adverse event.  The BCP covers the actions taken by key personnel, resources, and services required to continue critical business processes and operations. This plan is intended to address extended business disruptions. The development of the DRP follows Azure Business Continuity and Disaster Recovery SOP.  The DRP covers the actions taken by key personnel, resources, and services required to continue critical technology processes and operations. This plan is intended to address extended service disruptions. The development of the DRP follows Azure Business Continuity and Disaster Recovery SOP.  These plans are followed by all technology services; however, the individual steps for recovery are stored separately by the owning service teams and hyperlinks to each team's plans are provided to the BCM team for verification. The BCP and DRP document all program requirements and standard operating procedures used by all services covering all commonly shared processes. The individual service plans are the details of how a service recovers regardless of outage scope that can be followed by any authorized member of a service team. This allows Azure to eliminate single points of failure and ensures continuity of operations. |
| **Part B**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for distributing the contingency plans.  **Azure**  Microsoft distributes the BCP and DRP to all personnel via SharePoint. Service plans are stored on service-team-internal SharePoint sites, Wikis, or OneNote with links to them present in the Business Continuity Disaster Recovery (BCDR) Program section of the Azure Global Portal. Service teams are responsible for distributing service plans. |
| **Part C**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for coordinating contingency planning with incident handling.  **Azure**  Microsoft coordinates contingency planning with incident handling for Azure services as defined in the Azure Incident Management Standard Operating Procedure (SOP). Security and availability incidents are closely intertwined with business continuity and disaster recovery processes. |
| **Part D**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for reviewing the contingency plan.  **Azure**  Microsoft reviews the BCP and DRP for Azure services by following the policies defined in the Azure Business Continuity and Disaster Recovery SOP. These polices ensure plans are reviewed on at least on an annual basis by the Azure BCM team. Service teams are required to revalidate the BCDR Program section of the Azure Global Portal on an annual basis as well. Any service team contingency plans not meeting Azure standards are rejected for re-work and have to be resubmitted. |
| **Part E**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for updating the contingency plan and how those updates reflect changes to the organization, resources, or environment of operation; and the problems encountered during implementation, execution, or testing of contingency activities.  **Azure**  Microsoft updates the BCP and DRP on an annual basis and to address changes to the organization, information system, or environment of operation and problems encountered during plan implementation, execution, or testing. Reviews are conducted by the Azure BCM team, following the policies defined in the Azure Business Continuity and Disaster Recovery SOP. Service teams are required to revalidate the BCDR Program section of the Azure Global Portal on an annual basis as well. Any service team contingency plans not meeting Azure standards are rejected for re-work and have to be resubmitted. |
| **Part F**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for communicating changes made to the contingency plan.  **Azure**  Microsoft updates all plans for Azure services, following the policies defined in tAzure Business Continuity and Disaster Recovery SOP, including notifications to personnel via email, SharePoint, the BCDR Program in the Azure Global Portal, and service-team-specific notifications. |
| **Part G**  **Customer Responsibility**  The customer is responsible for incorporating lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training for customer-deployed resources.  **Azure**  Microsoft updates the BCP and DRP on an annual basis and to address changes to the organization, information system, or environment of operation and problems encountered during plan implementation, execution, or testing. Reviews are conducted by the Azure BCM team, following the policies defined in the Azure Business Continuity and Disaster Recovery SOP. Service teams are required to revalidate the BCDR Program section of the Azure Global Portal on an annual basis as well. Any service team contingency plans not meeting Azure standards are rejected for re-work and have to be resubmitted. Service teams are responsible for onboarding to BCDR Manager. Lessons learned from BCDR assessments are incorporated for future testing by service teams. |
| **Part H**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for protecting the contingency plan to prevent unauthorized disclosure or modification of the plan.  **Azure**  Microsoft protects the DRP, BCP, and service-specific plans for Azure services from unauthorized disclosure and modification. This is accomplished using SharePoint and Azure Global Portal access controls. Training and the Employee Agreement protect against the disclosure of information by Azure personnel. |

### CP-2(1) - Coordinate with Related Plans

Coordinate contingency plan development with organizational elements responsible for related plans.

|  |
| --- |
| **CP-2(1) Control Summary Information** |
| Responsible Roles: BCDR |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CP-2(1) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for coordinating contingency plan development with organizational elements responsible for related plans (e.g., business continuity, disaster recovery).  **Azure**  Following Azure Business Continuity and Disaster Recovery SOP, Azure has implemented the Azure Business Continuity Plan (BCP) and Azure Disaster Recovery Plan (DRP) which provide guidance and detailed procedures for recovery of Azure business operations. These documents address the purpose, scope, roles, responsibilities, compliance requirements, and required coordination among the various Microsoft organizations providing support for the security of Azure. The business continuity process contains a strategy for the recovery of Azure assets and the resumption of key Azure business processes. These contingency planning procedures are in accordance with NIST Special Publication 800-34 Revision 1, Contingency Planning Guide for Federal Information Systems. Additionally, Microsoft has created the Azure Incident Management Standard Operating Procedure (SOP), which supports and leveraged by the Azure BCP, DRP, and contingency planning procedures specific to Azure. |

### CP-2(2) - Capacity Planning

Conduct capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.

|  |
| --- |
| **CP-2(2) Control Summary Information** |
| Responsible Roles: Datacenter Hosting |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CP-2(2) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for conducting capacity planning to ensure customer-deployed resources continue operating during contingency activities. Note: if the customer configures Azure appropriately for reserving processing capacity in an alternate region, Azure can support continued system operation during contingency activities.  **Azure**  Azure implements a capacity planning process that ensures adequate resources are available for the Azure environment. The capacity management process includes the determination of the overall size, performance and resilience of the system. The capacity management process includes the following activities:  \* Understanding the current demands and forecasting the future requirements  \* Monitoring performance and throughput of services and supporting infrastructure components  \* Carry out tuning activities to ensure efficient utilization of available resources  \* Establishing and enforcing the policy for platform services contingency capacity buffer |

### CP-2(3) - Resume Mission and Business Functions

Plan for the resumption of [Selection: all;essential] mission and business functions within [time period defined in service provider and organization SLA] of contingency plan activation.

|  |
| --- |
| **CP-2(3) Control Summary Information** |
| Responsible Roles: BCDR |
| Parameter cp-02.03\_odp.01: all |
| Parameter cp-02.03\_odp.02: service Recovery Time Objectives (RTOs) documented in BCPs |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CP-2(3) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for resuming essential mission and business functions once contingency activities have commenced. Note: if the customer configures Azure appropriately for reserving processing capacity in an alternate region, Azure can support continued system operation during contingency activities.  **Azure**  Azure establishes a Recovery Time Objectives (RTO) for each Azure service and documents those RTOs as part of the BCM process. This process ensures services provided by Microsoft can resume all missions and business functions within the defined RTO. These RTOs align with all time periods defined in SLAs with customers. |

### CP-2(5) - Continue Mission and Business Functions

Plan for the continuance of [Selection: all;essential] mission and business functions with minimal or no loss of operational continuity and sustains that continuity until full system restoration at primary processing and/or storage sites.

|  |
| --- |
| **CP-2(5) Control Summary Information** |
| Responsible Roles: Datacenter Hosting, BCDR |
| Parameter cp-02.05\_odp: essential |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CP-2(5) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for continuing essential mission and business functions with little or no loss of operational continuity and sustain that continuity until full resource restoration has occurred at primary processing and/or storage sites for all customer-deployed resources. Note: if the customer configures Azure appropriately for reserving processing capacity in an alternate region, Azure can support continued system operation during contingency activities.  **Azure**  Azure plans for the continuance of essential missions and business functions by establishing alternate storage and processing sites at geographically-distributed Azure datacenters. Data is replicated between primary and alternate sites automatically, depending on the region recovery classification of the service. Azure does not consider any given datacenter or region as alternate - all sites are equally primary, and services determine the level of resiliency required. All sites have equivalent physical and logical security safeguards. |

### CP-2(8) - Identify Critical Assets

Identify critical system assets supporting [Selection: all;essential] mission and business functions.

|  |
| --- |
| **CP-2(8) Control Summary Information** |
| Responsible Roles: BCDR |
| Parameter cp-02.08\_odp: all |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CP-2(8) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for identifying critical customer-deployed resources.  **Azure**  Microsoft establishes recovery time objectives (RTO) for all Azure services and documents those RTOs as part of the BCM process. Essential services are defined as those with an RTO of 168 hours or less. |

## CP-3 Contingency Training

a. Provide contingency training to system users consistent with assigned roles and responsibilities:

1. Within [\\*See Additional Requirements] of assuming a contingency role or responsibility;

2. When required by system changes; and

3. [at least annually] thereafter; and

b. Review and update contingency training content [at least annually] and following [events necessitating review and update of contingency training are defined;].

(a) Requirement: Privileged admins and engineers must take the basic contingency training within 10 days. Consideration must be given for those privileged admins and engineers with critical contingency-related roles, to gain enough system context and situational awareness to understand the full impact of contingency training as it applies to their respective level. Newly hired critical contingency personnel must take this more in-depth training within 60 days of hire date when the training will have more impact.

|  |
| --- |
| **CP-3 Control Summary Information** |
| Responsible Roles: BCDR |
| Parameter cp-03\_odp.01: ten (10) days |
| Parameter cp-03\_odp.02: at least annually |
| Parameter cp-03\_odp.03: at least annually |
| Parameter cp-03\_odp.04: significant changes |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CP-3 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for providing contingency training to users of customer-deployed resources in accordance with assigned roles and responsibilities. The customer is also responsible for providing contingency retraining to users of customer-deployed resources, when changes occur, in accordance with assigned roles and responsibilities  **Azure**  Within ten (10) days of personnel taking on contingency roles and responsibilities, Azure ensures that required contingency training takes place. All personnel with a contingency planning role receive training on an annual basis, defined as a rolling three hundred and sixty five (365) days from the last training date. Upon completion of the training, personnel certify that they have been trained electronically and the training is stored and managed automatically by the BCDR Program training tool in the Azure Global Portal. The process is documented in the Azure Business Continuity and Disaster Recovery Standard Operating Procedure (SOP). Evidence of training is stored in BCDR Program training tool in the Azure Global Portal.Services with contingency staff who have not completed training are automatically notified and service remains non-compliant with BCDR program reviews until completed. Service team BCP owners and crisis communications managers receive training by participating in simulated events, including regular recovery testing and disaster recovery drills, as well as the training course within the BCDR Program training tool in the Azure Global Portal. This training occurs at least annually and prior to assuming a contingency-related role, as well as whenever system changes occur. |
| **Part B**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for reviewing and updating contingency training content at a defined frequency for defined events relating to customer-deployed resources.  **Azure**  Service team BCP owners and crisis communications managers receive training by participating in simulated events, including regular recovery testing and disaster recovery drills, as well as the training course within the BCDR Program training tool in the Azure Global Portal. This training occurs at least annually and prior to assuming a contingency-related role, as well as whenever system changes occur. The training content is reviewed and updated if necessary on at least annual basis by BCDR leads. |

### CP-3(1) - Simulated Events

Incorporate simulated events into contingency training to facilitate effective response by personnel in crisis situations.

|  |
| --- |
| **CP-3(1) Control Summary Information** |
| Responsible Roles: BCDR |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CP-3(1) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for facilitating effective response by personnel in crisis situations by incorporating simulated events into contingency training.  **Azure**  Azure includes LiveSite exercises and functional failover tests in training for personnel with contingency planning and recovery responsibilities. The objective of these exercises is to maximize plan accuracy and team preparedness to respond to incidents. Microsoft injects faults during testing to ensure successful recovery, allowing teams to respond to simulated incidents. |

## CP-4 Contingency Plan Testing

a. Test the contingency plan for the system [at least annually] using the following tests to determine the effectiveness of the plan and the readiness to execute the plan: [functional exercises].

b. Review the contingency plan test results; and

c. Initiate corrective actions, if needed.

(a) Requirement: The service provider develops test plans in accordance with NIST Special Publication 800-34 (as amended); plans are approved by the JAB/AO prior to initiating testing.

(b) Requirement: The service provider must include the Contingency Plan test results with the security package within the Contingency Plan-designated appendix (Appendix G, Contingency Plan Test Report).

|  |
| --- |
| **CP-4 Control Summary Information** |
| Responsible Roles: BCDR |
| Parameter cp-4(a): C+AI Security and DCS teams coordinate to perform annual contingency plan testing at each datacenter consisting of separate classroom material followed by a tabletop exercise based on an agreed upon scenario. Additional functional exercises (e.g. electrical systems) are performed around scheduled maintenance. |
| Parameter cp-04\_odp.01: at least annually |
| Parameter cp-04\_odp.02: |
| Parameter cp-04\_odp.03: |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CP-4 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for testing the contingency plan for customer-deployed resources.  **Azure**  Each service team performs tests to exercise their scenario listed in the Azure Business Continuity Plan (BCP) and Azure Disaster Recovery Plan (DRP) annually. These include every component and critical process listed in the Azure BCP and DRP. Also, functional exercises are completed in real time on an ongoing basis as incidents occur. |
| **Part B**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for reviewing the results of contingency plan testing (see CP-04.a).  **Azure**  Service teams create testing reports for all BCDR tests, are reviewed by the BCDR team, and entered into the BCDR Program in the Azure Global Portal. The BCDR team ensures that testing happens as per the defined schedule. |
| **Part C**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for initiating corrective action regarding contingency plan testing.  **Azure**  As a result of the testing performed, the Drill team, in conjunction with the BCDR team and service teams, reviews supporting evidence documented in the BCDR Program in the Azure Global Portal and in work items in Azure DevOps and identifies improvement opportunities for short, medium, and long-term follow-up. If critical issues are identified during an exercise, they are worked on until resolution, and BCDR documentation is updated accordingly as needed. The overall readiness of the BCP and DRP includes the readiness to execute the plan per the test results.  Azure assesses the effects on organizational operations and assets for every test exercise. The appropriate service team updates BCDR documentation for any issue identified. |

### CP-4(1) - Coordinate with Related Plans

Coordinate contingency plan testing with organizational elements responsible for related plans.

|  |
| --- |
| **CP-4(1) Control Summary Information** |
| Responsible Roles: BCDR |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CP-4(1) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for coordinating contingency plan testing with the testing of related plans (e.g., business continuity, disaster recovery).  **Azure**  Service teams conduct BCDR assessments on at least annual basis which is designed to test contingency procedures. The BCDR team is engaged in analysis and actions based on results. All Azure datacenters can be used as alternate processing sites, and each site has the necessary agreements in place to transfer and resume services logically without equipment transfer. |

### CP-4(2) - Alternate Processing Site

Test the contingency plan at the alternate processing site:

(a) To familiarize contingency personnel with the facility and available resources; and

(b) To evaluate the capabilities of the alternate processing site to support contingency operations.

|  |
| --- |
| **CP-4(2) Control Summary Information** |
| Responsible Roles: BCDR |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CP-4(2) What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for testing the contingency plan at an alternate processing location to familiarize contingency personnel with the facility and resources available at the alternate site. Note: if the customer configures Azure appropriately for reserving processing capacity in an alternate region, Azure can support contingency testing and provide continued system operation during contingency activities.  **Azure**  All Azure sites have dedicated personnel and equivalent capabilities, ensuring contingency personnel are familiar with the facility and available resources as a part of normal job functions. |
| **Part B**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for testing and evaluating the contingency plan at an alternate processing site to support contingency operations. Note: if the customer configures Azure appropriately for reserving processing capacity in an alternate region, Azure can support contingency testing and provide continued system operation during contingency activities.  **Azure**  All Azure sites have dedicated personnel and equivalent capabilities, ensuring contingency personnel are familiar with the facility and available resources as a part of normal job functions. |

## CP-6 Alternate Storage Site

a. Establish an alternate storage site, including necessary agreements to permit the storage and retrieval of system backup information; and

b. Ensure that the alternate storage site provides controls equivalent to that of the primary site.

|  |
| --- |
| **CP-6 Control Summary Information** |
| Responsible Roles: Datacenter Hosting, BCDR |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CP-6 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for establishing an alternate storage site with the ability to store and retrieve backup information, and the agreements permitting such activities. Note: if the customer configures Azure appropriately for reserving storage capacity in an alternate region, Azure can support the secure storage and retrieval of system data.  **Azure**  Azure establishes alternate storage sites at geographically distributed Azure datacenters, including all agreements to permit storage and retrieval of information. In addition, each Azure service provides the capabilities and guidance for replication of data to alternate storage sites and seamless failover. |
| **Part B**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for establishing an alternate storage site with equivalent security safeguards as the primary site. Note: if the customer configures Azure appropriately for reserving storage capacity in an alternate region, Azure can support the secure storage and retrieval of system data.  **Azure**  All storage sites are Azure datacenters with equivalent security safeguards. |

### CP-6(1) - Separation from Primary Site

Identify an alternate storage site that is sufficiently separated from the primary storage site to reduce susceptibility to the same threats.

|  |
| --- |
| **CP-6(1) Control Summary Information** |
| Responsible Roles: Datacenter Hosting, BCDR |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CP-6(1) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for establishing an alternate storage site that is separate from the primary storage site to reduce its susceptibility to the same threats (e.g., natural disasters). Note: if the customer configures Azure appropriately for reserving storage capacity in an alternate region, Azure can support the secure storage and retrieval of system data.  **Azure**  Alternate storage sites in the form of Azure datacenters are geographically separated so as not to be susceptible to the same threats. The Azure authorization boundary currently consists of fully managed and leased datacenters across geographically separated locations. |

### CP-6(2) - Recovery Time and Recovery Point Objectives

Configure the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives.

|  |
| --- |
| **CP-6(2) Control Summary Information** |
| Responsible Roles: Datacenter Hosting, BCDR |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CP-6(2) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for establishing an alternate storage site that facilitates recovery operations consistent with customer-defined recovery time objectives (RTO's) and recovery point objectives (RPO's). Note: if the customer configures Azure appropriately for reserving storage capacity in an alternate region, Azure can support the secure storage and retrieval of system data.  **Azure**  Due to the fully redundant architecture of Azure as described in the Azure Business Continuity Plan (BCP) and Azure Disaster Recovery Plan (DRP), alternate storage sites in the form of Azure datacenters are designed and implemented to be continuously available. Site availability does not impact the RTO or RPO for any given Azure service due to the redundant architecture. |

### CP-6(3) - Accessibility

Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions.

|  |
| --- |
| **CP-6(3) Control Summary Information** |
| Responsible Roles: Datacenter Hosting, BCDR |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CP-6(3) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for identifying potential issues and mitigating actions to ensure accessibility to the established alternative storage site during disruption or disaster. Note: if the customer configures Azure appropriately for reserving storage capacity in an alternate region, Azure can support the secure storage and retrieval of system data.  **Azure**  Azure manages all datacenters and has Emergency Management Teams (EMTs) in place to discuss with all team members any accessibility problems to datacenters in the event of an area-wide disruption or disaster and details explicit mitigation actions. If there is a disruption to any datacenter, Azure personnel from that site do not have to go to another datacenter, as there are Azure personnel already engaged and operating at all sites. An area-wide disruption or disaster at the primary site does not affect the Azure secondary site or sites since they are located in geographically separated regions for each system. Azure personnel are located throughout the United States, and have the capability to work remotely. |

## CP-7 Alternate Processing Site

a. Establish an alternate processing site, including necessary agreements to permit the transfer and resumption of [system operations for essential mission and business functions are defined;] for essential mission and business functions within [time period consistent with recovery time and recovery point objectives is defined;] when the primary processing capabilities are unavailable;

b. Make available at the alternate processing site, the equipment and supplies required to transfer and resume operations or put contracts in place to support delivery to the site within the organization-defined time period for transfer and resumption; and

c. Provide controls at the alternate processing site that are equivalent to those at the primary site.

(a) Requirement: The service provider defines a time period consistent with the recovery time objectives and business impact analysis.

|  |
| --- |
| **CP-7 Control Summary Information** |
| Responsible Roles: Datacenter Hosting, BCDR |
| Parameter cp-07\_odp.01: operations defined in the Azure Business Continuity Plan (BCP) |
| Parameter cp-07\_odp.02: recovery objectives defined in the Azure Business Continuity Plan (BCP) |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CP-7 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for establishing an alternate processing site with agreements permitting the transfer and resumption of customer-defined system operations consistent with customer-defined recovery time and recovery point objectives when the primary processing site is unavailable. Note: if the customer configures Azure appropriately for reserving processing capacity in an alternate region, Azure can support the continuation of secure system operation.  **Azure**  All Azure datacenters can be used as alternate processing sites, and each site has the necessary agreements in place to transfer and resume services logically without equipment transfer. Azure service teams determine recovery objectives following the Business Impact Analysis (BIA) process and services are designed and tested to meet objectives, following the Azure Business Continuity Management (BCM) process. |
| **Part B**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for establishing an alternate processing site with the resources and ability to transfer and resume operations within the time period defined in CP-07.a. Note: if the customer configures Azure appropriately for reserving processing capacity in an alternate region, Azure can support the continuation of secure system operation. Customer and Microsoft ResponsibilitiesMicrosoft takes an infrastructure approach to disaster recovery, providing the capabilities required for customers to implement the recovery appropriate for their business. Customers must follow the appropriate guidance to ensure correct implementation of their business continuity solution. For example, to protect Azure Storage data from a region wide disaster storage accounts must be configured to use geo-replication (GRS or RA-GRS).  **Azure**  All Azure datacenters can be used as alternate processing sites, and each site has the necessary agreements in place to transfer and resume services logically without equipment transfer. The BCDR Program in the Azure Global Portal explicitly covers business processes defined during the BIA with Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for each service. |
| **Part C**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for establishing an alternate processing site that has security safeguards equivalent to the primary site. Note: if the customer configures Azure appropriately for reserving processing capacity in an alternate region, Azure can support the continuation of secure system operation.  **Azure**  As Azure datacenters, Azure’s alternate data processing sites have equivalent physical and logical security safeguards in place. |

### CP-7(1) - Separation from Primary Site

Identify an alternate processing site that is sufficiently separated from the primary processing site to reduce susceptibility to the same threats.

Guidance: The service provider may determine what is considered a sufficient degree of separation between the primary and alternate processing sites, based on the types of threats that are of concern. For one particular type of threat (i.e., hostile cyber attack), the degree of separation between sites will be less relevant.

|  |
| --- |
| **CP-7(1) Control Summary Information** |
| Responsible Roles: Datacenter Hosting, BCDR |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CP-7(1) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for establishing an alternative processing site that is separate from the primary processing site to reduce its susceptibility to the same threats (e.g., natural disasters). Note: if the customer configures Azure appropriately for reserving processing capacity in an alternate region, Azure can support the continuation of secure system operation.  **Azure**  As Azure datacenters, alternate processing sites are geographically separated so as not to be susceptible to the same threats. The Azure authorization boundary currently consists of fully managed and leased datacenters across geographically separated locations. |

### CP-7(2) - Accessibility

Identify potential accessibility problems to alternate processing sites in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

|  |
| --- |
| **CP-7(2) Control Summary Information** |
| Responsible Roles: BCDR |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CP-7(2) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for identifying issues and mitigating actions to ensure accessibility to the established alternative processing site during disruption or disaster. Note: if the customer configures Azure appropriately for reserving processing capacity in an alternate region, Azure can support the continuation of secure system operation.  **Azure**  Azure manages all datacenters and has Emergency Management Teams (EMTs) in place to discuss with all team members any accessibility problems to datacenters in the event of an area-wide disruption or disaster and details explicit mitigation actions. If there is a disruption to any datacenter, Azure personnel from that site do not have to go to another datacenter, as there are Azure personnel already engaged and operating at all sites. An area-wide disruption or disaster at the primary site does not affect the Azure secondary site or sites since they are located in geographically separated regions for each system. Azure personnel are located throughout the United States, and have the capability to work remotely. |

### CP-7(3) - Priority of Service

Develop alternate processing site agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives).

|  |
| --- |
| **CP-7(3) Control Summary Information** |
| Responsible Roles: Datacenter Hosting, BCDR |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CP-7(3) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for establishing alternate processing site agreements containing priority-of-service provisions which correspond with customer-defined availability requirements (e.g., RTO's). Note: if the customer configures Azure appropriately for reserving processing capacity in an alternate region, Azure can support the continuation of secure system operation.  **Azure**  Azure is located within Azure datacenters. Azure is responsible for managing all alternate processing sites for Azure; therefore, it is not necessary for site agreements to be in place. Priority-of-service provisions are not required because Azure owns and manages or leases all datacenter facilities for Azure.  Microsoft establishes recovery time objectives (RTO) for all Azure services and documents those RTOs as part of the BCM process. Essential services are defined as those with an RTO of 168 hours or less. These RTOs serve as the alternate processing site agreements which determine the priority-of-service provisions for each Azure service. |

### CP-7(4) - Preparation for Use

Prepare the alternate processing site so that the site can serve as the operational site supporting essential mission and business functions.

|  |
| --- |
| **CP-7(4) Control Summary Information** |
| Responsible Roles: Datacenter Hosting, BCDR |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CP-7(4) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for preparing the alternate processing site to be used as the operational site supporting essential missions and business functions. Note: if the customer configures Azure appropriately for reserving processing capacity in an alternate region, Azure can support the continuation of secure system operation.  **Azure**  Azure deploys services in redundant configurations. Azure datacenters functioning as alternate sites are always ready to be used as operational sites supporting all missions and business functions. |

## CP-8 Telecommunications Services

Establish alternate telecommunications services, including necessary agreements to permit the resumption of [system operations to be resumed for essential mission and business functions are defined;] for essential mission and business functions within [time period within which to resume essential mission and business functions when the primary telecommunications capabilities are unavailable is defined;] when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

Requirement: The service provider defines a time period consistent with the recovery time objectives and business impact analysis.

|  |
| --- |
| **CP-8 Control Summary Information** |
| Responsible Roles: Fiber |
| Parameter cp-08\_odp.01: all information system operations |
| Parameter cp-08\_odp.02: recovery time objectives (RTOs) identified in the Azure Business Continuity Plan (BCP) |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CP-8 What is the solution and how is it implemented?** |
| **Azure**  Azure is responsible for ensuring continuity of its telecommunications services through the process of utilizing diverse fiber routes and redundant hardware to provide maximum availability at each site. Each Site represented as part of the Azure boundary is active, independent from all other sites, and fully operational with the ability to provide services at any time. Critical problems are defined as incidents or outages, other than caused by an Excused Outage, which cause a Microsoft Equipment failure, as a result of which Microsoft cannot receive any data.  In addition to the active site configuration, and as an ISP whose purpose is to exclusively host online services, Azure maintains a global fiber backbone comparable to multiple commercial ISPs. Some fiber routes have triple redundancy but all have a minimum of double redundancy. Azure contracts for the fiber paths are dedicated to Microsoft. Microsoft engages and contracts with providers to provide field service maintenance in the event of faults, defects, or failures. |

### CP-8(1) - Priority of Service Provisions

(a) Develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives); and

(b) Request Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness if the primary and/or alternate telecommunications services are provided by a common carrier.

|  |
| --- |
| **CP-8(1) Control Summary Information** |
| Responsible Roles: Fiber |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CP-8(1) What is the solution and how is it implemented?** |
| **Part A**  **Azure**  Network routing for Azure datacenters is proprietary, and therefore a Service Priority setting for emergency purposes is not required. Azure is responsible for defining its own routing priority based on property availability requirements and emergency purposes. In the cloud environment, there is no priority order because there are different teams to bring each specific component back online in the Recovery Time Objectives (RTOs) defined for each service. Azure can define its own routing priority based on Property availability requirements and emergency purposes. |
| **Part B**  **Azure**  Network routing for Azure datacenters is proprietary, and therefore a Service Priority setting for emergency purposes is not required. Azure is responsible for defining its own routing priority based on property availability requirements and emergency purposes. In the cloud environment, there is no priority order because there are different teams to bring each specific component back online in the Recovery Time Objectives (RTOs) defined for each service. Azure can define its own routing priority based on Property availability requirements and emergency purposes. |

### CP-8(2) - Single Points of Failure

Obtain alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.

|  |
| --- |
| **CP-8(2) Control Summary Information** |
| Responsible Roles: Fiber |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CP-8(2) What is the solution and how is it implemented?** |
| **Azure**  Azure mitigates the risk of single points of failures with telecommunication links by requiring each Azure datacenter to have at least two (2) diverse fiber paths. Microsoft maintains its own fiber network whose purpose is to exclusively support Microsoft properties, acting as a global fiber backbone comparable to multiple ISPs. Azure contracts with multiple carriers to provide field service maintenance in the event of faults, defects, or failures. The service level objective with the carriers for on-demand maintenance and critical time to repair is twenty-four (24) hours. |

### CP-8(3) - Separation of Primary and Alternate Providers

Obtain alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats.

|  |
| --- |
| **CP-8(3) Control Summary Information** |
| Responsible Roles: Fiber |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CP-8(3) What is the solution and how is it implemented?** |
| **Azure**  Azure mitigates the risk of single points of failures with telecommunication links by requiring each Azure datacenter to have at least two (2) separate fiber paths. The redundant communication links are established following disparate paths through the Microsoft fiber network. This is a continuously operational solution managed by Azure. |

### CP-8(4) - Provider Contingency Plan

(a) Require primary and alternate telecommunications service providers to have contingency plans;

(b) Review provider contingency plans to ensure that the plans meet organizational contingency requirements; and

(c) Obtain evidence of contingency testing and training by providers [annually].

|  |
| --- |
| **CP-8(4) Control Summary Information** |
| Responsible Roles: Fiber |
| Parameter cp-8.4\_prm\_1: annually |
| Parameter cp-08.04\_odp.01: |
| Parameter cp-08.04\_odp.02: |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CP-8(4) What is the solution and how is it implemented?** |
| **Part A**  **Azure**  Azure does not rely on contingency plans for individual ISPs to maintain telecommunications. Microsoft implements diverse fiber routes that automatically transfer transmissions during outages. In addition, Microsoft has contracts and SLAs to ensure timely remediation of any issues. |
| **Part B**  **Azure**  Azure does not rely on contingency plans for individual ISPs to maintain telecommunications. Microsoft implements diverse fiber routes that automatically transfer transmissions during outages. In addition, Microsoft has contracts and SLAs to ensure timely remediation of any issues. |
| **Part C**  **Azure**  Azure does not rely on contingency plans for individual ISPs to maintain telecommunications. Microsoft implements diverse fiber routes that automatically transfer transmissions during outages. In addition, Microsoft has contracts and SLAs to ensure timely remediation of any issues. |

## CP-9 System Backup

a. Conduct backups of user-level information contained in [system components for which to conduct backups of user-level information is defined;] [daily incremental; weekly full];

b. Conduct backups of system-level information contained in the system [daily incremental; weekly full];

c. Conduct backups of system documentation, including security- and privacy-related documentation [daily incremental; weekly full] ; and

d. Protect the confidentiality, integrity, and availability of backup information.

Requirement: The service provider shall determine what elements of the cloud environment require the Information System Backup control. The service provider shall determine how Information System Backup is going to be verified and appropriate periodicity of the check.

(a) Requirement: The service provider maintains at least three backup copies of user-level information (at least one of which is available online) or provides an equivalent alternative.

(b) Requirement: The service provider maintains at least three backup copies of system-level information (at least one of which is available online) or provides an equivalent alternative.

(c) Requirement: The service provider maintains at least three backup copies of information system documentation including security information (at least one of which is available online) or provides an equivalent alternative.

|  |
| --- |
| **CP-9 Control Summary Information** |
| Responsible Roles: Storage |
| Parameter cp-09\_odp.01: persistent storage components |
| Parameter cp-09\_odp.02: daily incremental and weekly full; critical information and services are deployed in redundant regions in an active–active configuration |
| Parameter cp-09\_odp.03: daily incremental and weekly full; critical information and services are deployed in redundant regions in an active–active configuration |
| Parameter cp-09\_odp.04: daily incremental and weekly full; critical information and services are deployed in redundant regions in an active–active configuration |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CP-9 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for conducting backups of user-level information in customer-deployed resources at a frequency consistent with customer-defined RTO's and RPO's. Note: if the customer configures Azure backup services appropriately, Azure can support data loss prevention.  **Azure**  For user-level information stored in Azure Storage, data is synchronously replicated locally using Locally Redundant Storage (LRS), which provides redundancy equivalent to three copies. In addition, data is asynchronously replicated to a separate datacenter in the zone or to a remote region for accounts which have configured Zone-Redundant Storage (ZRS), Geo-Redundant Storage (GRS), or Read-Access Geo-Redundant Storage (RA-GRS). The backups sent to Azure Storage are encrypted using Federal Information Processing Standards (FIPS) 140-2 compliant AES 256-bit encryption. There are three types of backups – Customer Machine, Disk Pod, and Tape. For Customer Machine and Disk Pod backups, the data is tied together in a location and retained for seven (7) days. Disk Pods back up to Blob storage, in which there are two accounts, ensuring that data is backed up into two accounts in different regions. For tape backup, the Data Protection Services (DPS) policies and procedures describe the roles, responsibilities, and services for the backup standards, retention policies, monitoring, and reports available to customers.  All information backed up and stored uses the Data Type Classification according to the Corporate, External and Legal Affairs (CELA) Data Classification. Service teams are required to identify the Data Type Classification that in turn drives the appropriate retention and storage policy assigned.  The default settings include a full backup once a week and a nightly differential backup. If the backup schedule needs changing based on customer requirements, a workflow ticket is opened requesting the change. The ticket is reviewed and approved by DPS prior to instituting the change.  Backup tapes are moved to an off-site facility for long term storage. The scalar tape backup library, encryption device, and servers are in each applicable datacenter. The secure offsite backup process consists of the following:  \* Off-site containers are stored within the datacenter.  \* The containers are loaded within the datacenter by authorized personnel.  \* All tapes are placed inside the containers for transport.  \* Containers are locked by authorized personnel.  \* CommVault Simpana Software is used to track the tape numbers through a vault report. Along with the CommVault Simpana vault report, a workflow ticket is created to track the tapes, their transport, and the personnel involved. The tracking is to ensure location of the tapes in the event a recovery is requested.  \* The off-site vendor retrieves the containers according to a schedule specified by DPS.  \* The locked containers are stored within the datacenter until an off-site vendor representative can retrieve the tape containers.  \* When the off-site vendor picks up the tape containers, they are not allowed to enter any datacenter, as mandated by security. The tape containers are brought to the lobby for the exchange.  \* Authorized personnel who handle the tapes are required to have an authorization account with the off-site vendor. This account includes a unique account number that is tracked by the off-site vendor when tapes are exchanged.  \* If tapes need to be retrieved for recovery purposes, authorized personnel can request the tape from off-site storage.  All recovery requests are initiated by the customer by opening a workflow ticket. This ticket allows tracking of the entire recovery process. Expired tapes are tracked by vaulting and the off-site vendor. tapes are returned to the datacenter on the day of expiration. |
| **Part B**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for conducting backups of system-level information in customer-deployed resources at a frequency consistent with customer-defined RTO's and RPO's. Note: if the customer configures Azure backup services appropriately, Azure can support data loss prevention.  **Azure**  System-level information is backed up using Azure Storage continuous replication detailed above. System-level information, defined as system-state information, operating system and application software, and licenses, is maintained in a variety of ways, but are backed by Azure Storage, which utilizes LRS, ZRS, GRS. Server, network device, and service code is maintained in Azure DevOps, which is backed up and redundant. Azure DevOps uses Azure Storage as the primary repository for service metadata and data. For additional information on DevOps, please see the link below:  <https://docs.microsoft.com/en-us/azure/devops/organizations/security/data-protection?view=azure-devops#data-availability> |
| **Part C**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for conducting backups of system documentation information in customer-deployed resources at a frequency consistent with customer-defined RTO's and RPO's. Note: if the customer configures Azure backup services appropriately, Azure can support data loss prevention.  **Azure**  Information system documentation and security-related documentation are stored on SharePoint. SharePoint backups are managed by Core Services Engineering and Operations (CSEO). Backup frequency is based on requirements defined by the BIA. |
| **Part D**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for protecting the confidentiality, integrity, and availability (CIA) of customer-controlled backup data. Note: if the customer configures Azure backup services appropriately, Azure can support the protection of backup data.  **Azure**  Azure protects the confidentiality and integrity of all information in accordance with Federal Information Processing Standards (FIPS) 140-2 primarily through the automatic encryption of data uploaded to Azure Storage. In addition, communications between the Azure service offerings are configured to require Federal Information Processing Standards (FIPS) 140-2 compliant TLS 1.2/1.3. As part of the drive to ensure that Microsoft is only using cryptographically secure protocol versions, all teams within Azure are provided guidance to deprecate older protocols and ciphers. Service Teams are only allowed to leverage TLS 1.2/1.3 and higher protocols for both incoming and outgoing connections. Azure leverages Key Performance Indicator (KPI) alerting system to ensure service teams are only leveraging TLS 1.2/1.3 and higher protocols. The KPIs are alerted to Azure service and leadership teams for actions. Azure enforces key communications between Azure internal components to be protected with self-signed SSL certificates. |

### CP-9(1) - Testing for Reliability and Integrity

Test backup information [at least monthly] to verify media reliability and information integrity.

|  |
| --- |
| **CP-9(1) Control Summary Information** |
| Responsible Roles: Storage |
| Parameter cp-9.1\_prm\_1: at least monthly |
| Parameter cp-09.01\_odp.01: |
| Parameter cp-09.01\_odp.02: |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CP-9(1) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for backing up customer data and applications. The customer is also responsible for testing those backups. Additionally, as detailed below, the customer is responsible for requesting a test of the backup of their image as systemically created by the Azure DPS team.  **Azure**  Azure monitors all backups of the system and the customer images on a continuous basis using system-generated alerts which notify the Azure service teams of any failed or incomplete backups. Azure Storage automatically addresses backup issues as they arise. If a backup continuously fails, Azure creates an IcM incident ticket to track and resolve the issue. In addition to system-generated alerts, restoration tests of customer-requested restores are performed using the BCDR Program in the Azure Global Portal. The integrity of data is automatically confirmed upon completion of the backup. The restoration tests are captured and stored in the BCDR Program in the Azure Global Portal to generate reports and perform root-cause analysis, as needed.  In addition, Azure can test backups for information integrity by request from the customer. A workflow ticket must be submitted by the customer to initiate the request to test backups. |

### CP-9(2) - Test Restoration Using Sampling

Use a sample of backup information in the restoration of selected system functions as part of contingency plan testing.

|  |
| --- |
| **CP-9(2) Control Summary Information** |
| Responsible Roles: Storage |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CP-9(2) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for testing backup information. Note: if the customer configures Azure backup services appropriately, Azure can support the testing of backup information.  **Azure**  The nature of functional business continuity and disaster recovery (BCDR) testing ensures that the redundancy built into the annual BCDR service team testing is fully addressed. This redundancy includes using actual backup information in the form of redundant processing being tested. |

### CP-9(3) - Separate Storage for Critical Information

Store backup copies of [critical system software and other security-related information backups to be stored in a separate facility are defined;] in a separate facility or in a fire rated container that is not collocated with the operational system.

|  |
| --- |
| **CP-9(3) Control Summary Information** |
| Responsible Roles: Storage |
| Parameter cp-09.03\_odp: all operating system and critical software code |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CP-9(3) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for separately storing backup information (e.g., separate facility or fire-rated container that is not collocated). Note: if the customer configures Azure backup services appropriately, Azure can support the protection of backup data.  **Azure**  All Azure server, network device, and service code is backed up in Azure DevOps. Multiple backups exist in geo-diverse locations. All Azure datacenters can be used as alternate processing sites, and each site has the necessary agreements in place to transfer and resume services logically without equipment transfer. Azure service teams determine recovery objectives following the Business Impact Analysis (BIA) process and services are designed and tested to meet objectives, following the Azure Business Continuity Management (BCM) process. |

### CP-9(5) - Transfer to Alternate Storage Site

Transfer system backup information to the alternate storage site [time period and transfer rate consistent with the recovery time and recovery point objectives defined in the service provider and organization SLA.].

|  |
| --- |
| **CP-9(5) Control Summary Information** |
| Responsible Roles: Storage |
| Parameter cp-9.5\_prm\_1: in accordance with RTOs and RPOs defined in the Azure Business Continuity Plan (BCP) |
| Parameter cp-09.05\_odp.01: |
| Parameter cp-09.05\_odp.02: |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CP-9(5) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for transferring backup information to an alternate storage site. Note: if the customer configures Azure backup services appropriately, Azure can support the storage of backup data.Azure automatically copies the backups of the customer data to the storage site within the same datacenter. These backups are automatically geo-replicated to the alternative storage site in different geographic regions.If the datacenter hosting the customer data fails, the customer can utilize the Azure Management Portal or programmatic API to restore their data from the geo-replicated backup to any geographic region of their choice.Additional information about how customers can submit a geo-restore request can be found here: <http://msdn.microsoft.com/en-us/library/azure/dn715779.aspx>. In the case of failure at the customer’s primary datacenter, the customer is responsible for restoring their data from backups to an alternative datacenter.  **Azure**  Azure establishes alternate storage sites at geographically distributed Azure datacenters. Data durability is obtained by synchronously replicating data across different databases in the same datacenter and across multiple datacenters. Disaster recovery is achieved by asynchronous replication to a datacenter in a different geographical region. Azure datacenters are redundant and services are mirrored in geographically redundant datacenters. All sites are active and both sites in a redundant pair contain the backed-up data. |

### CP-9(8) - Cryptographic Protection

Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of [all backup files].

Guidance: Note that this enhancement requires the use of cryptography which must be compliant with Federal requirements and utilize FIPS validated or NSA approved cryptography (see SC-13.)

|  |
| --- |
| **CP-9(8) Control Summary Information** |
| Responsible Roles: Storage |
| Parameter cp-09.08\_odp: all backup files |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CP-9(8) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for implementing cryptographic mechanisms to prevent unauthorized disclosure and modification of defied backup information housed in customer-deployed resources.  **Azure**  Azure protects the confidentiality and integrity of all information in accordance with Federal Information Processing Standards (FIPS) 140-2 primarily through the automatic encryption of data uploaded to Azure Storage. In addition, communications between the Azure service offerings are configured to require Federal Information Processing Standards (FIPS) 140-2 compliant TLS 1.2/1.3. As part of the drive to ensure that Microsoft is only using cryptographically secure protocol versions, all teams within Azure are provided guidance to deprecate older protocols and ciphers. Service Teams are only allowed to leverage TLS 1.2/1.3 and higher protocols for both incoming and outgoing connections. Azure leverages Key Performance Indicator (KPI) alerting system to ensure service teams are only leveraging TLS 1.2/1.3 and higher protocols. The KPIs are alerted to Azure service and leadership teams for actions. Azure enforces key communications between Azure internal components to be protected with self-signed SSL certificates. |

## CP-10 System Recovery and Reconstitution

Provide for the recovery and reconstitution of the system to a known state within [Assignment: organization-defined time period consistent with recovery time and recovery point objectives] after a disruption, compromise, or failure.

|  |
| --- |
| **CP-10 Control Summary Information** |
| Responsible Roles: Datacenter Hosting, Storage, BCDR |
| Parameter cp-10: in accordance with RTOs and RPOs defined in the Azure Business Continuity Plan (BCP) |
| Parameter cp-10\_odp.01: |
| Parameter cp-10\_odp.02: |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CP-10 What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for the recovery and reconstitution of customer-deployed resources after a disruption, compromise, or failure. Note: if the customer configures Azure backup and/or alternate site processing services appropriately, Azure can support the continued operation of customer-deployed resources.  **Azure**  All services are designed to be as redundant as needed by their region recovery classification. Because of this redundancy, the main recovery and reconstitution actions would take place at the damaged datacenter. Following an assessment of the damage to the datacenter, Azure plans a date for relocation of services using a phased approach. Azure prepares a schedule detailing when particular services are to relocate back to the rebuilt datacenter. Some key factors that are considered when scheduling the move are:  \* Ensuring the necessary core platforms and communications links are in place before restoration of the individual service teams.  \* Ensuring the supported tools are in place to support restoration.  \* Where different services are interdependent (e.g., data is passed to/from the services), restoring them to a consistent point in time and relocating them together.  A detailed checklist for recovery and reconstitution of the datacenter can be found in the Datacenter Business Resilience Plan (DC BRP). Each datacenter has its own unique DC BRP. |

### CP-10(2) - Transaction Recovery

Implement transaction recovery for systems that are transaction-based.

|  |
| --- |
| **CP-10(2) Control Summary Information** |
| Responsible Roles: Storage |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CP-10(2) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for implementing transaction-based (e.g., transaction rollback, transaction journaling) recovery within customer-deployed resources. Note: if the customer configures Azure backup and/or alternate site processing services appropriately, Azure can support the continued operation of customer-deployed resources.  **Azure**  Currently there are no transaction-based systems in the Azure environment. The primary and alternate sites are operational, management, and technical mirrors. Therefore, the need to recover and reconstitute information systems during significant contingency events is eliminated. Instead of using transaction journaling, Azure uses live replicated databases. MySQL uses transaction journaling while Microsoft SQL uses transaction logs. Transaction logging is a core function of the SQL engine and cannot be disabled. Common practice at Microsoft is replicate the transaction log to multiple assets and replay them to keep hot standby secondary databases on those assets up to date. This mechanism is referred to as Always On. Always On maintains multiple copies of a single database that reside on different server instances in different locations. One server instance serves the database to clients (the primary server). The other instance acts as a hot or warm standby server. In the event of a disaster, a failover quickly brings the standby copy of the database online (without data loss). For an Overview of SQL Server Always On, please refer to <https://docs.microsoft.com/en-us/sql/database-engine/availability-groups/windows/overview-of-always-on-availability-groups-sql-server>. Therefore, this is an alternative to transaction journaling because it provides the means to provide support for contingency events. Also, per Microsoft "10.01 Business Continuity Management Standard", transaction recovery plans are required and managed by the different business groups to ensure the continuation of business processes in the event of an interruption. |

### CP-10(4) - Restore Within Time Period

Provide the capability to restore system components within [time period consistent with the restoration time-periods defined in the service provider and organization SLA] from configuration-controlled and integrity-protected information representing a known, operational state for the components.

|  |
| --- |
| **CP-10(4) Control Summary Information** |
| Responsible Roles: Datacenter Hosting, BCDR |
| Parameter cp-10.04\_odp: |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **CP-10(4) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for restoring customer-deployed resources to a configuration-controlled and integrity-protected known, operational state. Note: if the customer configures Azure backup and/or alternate site processing services appropriately, Azure can support the continued operation of customer-deployed resources.  **Azure**  If all datacenters for an Azure service experience failure, or if Microsoft were to resume processing at a disrupted site, Microsoft uses the following to recover Azure services in other Azure datacenters to the last known state:  \* Defined images and current OS, network device, and application baselines  \* Defined security processes around access control, change management, mandatory configuration settings, and encryption mechanisms  Redeployment as part of system restoration follows the same process with the same authentication requirements as initial deployment as part of configuration management.  Azure does not establish separate recovery times for individual datacenter components due to the design and function of datacenters. Azure datacenters are designed to be redundant by hosting services in datacenters that are geographically separated from each other. Services are mirrored in geographically redundant datacenters; all sites are active. Therefore, the risk to the security of the Azure environment due to failure of individual components is mitigated through availability of the information system.  If necessary to support the resumption of a service according to the established Azure Disaster Recovery Plan (DRP), individual system components are replaced in support of the service Recovery Time Objective (RTO). The Azure spares policy ensures that spare components are available if replacement is needed. |

# Identification and Authentication (IA)

## IA-1 Policy and Procedures

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (OneOrMore): organization-level;mission/business process-level;system-level] identification and authentication policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the identification and authentication policy and the associated identification and authentication controls;

b. Designate an [an official to manage the identification and authentication policy and procedures is defined;] to manage the development, documentation, and dissemination of the identification and authentication policy and procedures; and

c. Review and update the current identification and authentication:

1. Policy [at least annually] and following [events that would require the current identification and authentication policy to be reviewed and updated are defined;] ; and

2. Procedures [at least annually] and following [significant changes].

|  |
| --- |
| **IA-1 Control Summary Information** |
| Responsible Roles: SOP Team, Policy |
| Parameter ia-1(a): all personnel |
| Parameter ia-01\_odp.01: |
| Parameter ia-01\_odp.02: |
| Parameter ia-01\_odp.03: a Microsoft-wide |
| Parameter ia-01\_odp.04: the Microsoft Information Risk Management Council (IRMC) organization |
| Parameter ia-01\_odp.05: at least annually |
| Parameter ia-01\_odp.06: significant changes |
| Parameter ia-01\_odp.07: at least annually |
| Parameter ia-01\_odp.08: significant changes |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☒ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **IA-1 What is the solution and how is it implemented?** |
| **Part A1**  **Customer Responsibility**  The customer is responsible for developing, documenting, and disseminating identification and authentication policy and procedures that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.  **Azure**  Azure addresses the identification and authentication policy as part of the Microsoft security policies, of which there are two sets: the Microsoft Security Policy (MSP) that is applicable to all Microsoft personnel, and the Microsoft Security Program Policy (MSPP), which is applicable to all Microsoft personnel that have a responsibility for security. The Microsoft Information Risk Management Council (IRMC) is the governance body with review and approval responsibility for the MSP and MSPP. Within Azure, the MSPP specifically applies to all Microsoft personnel with security objectives such as designing, building, and operating Azure and across all information and processes used in the conduct of Microsoft business. All Azure personnel are accountable and responsible for complying with these guiding principles within their designated roles. The policy addresses the following:  \* Identification and authentication of users and components  \* Unique identifiers  \* Default user accounts  Additionally, the policy addresses the purpose, scope, roles, responsibilities, compliance requirements, and required coordination among the various Microsoft organizations that provide some level of support to all services. The policies indicate Microsoft management’s commitment and are a component of the risk management strategy which provides Azure personnel with a current set of clear and concise information security requirements.  The MSP is available to all Microsoft personnel on the Microsoft Policy website on the Microsoft intranet, and the MSPP and Security Standards are available through the Liquid tool, also on the Microsoft intranet. The Azure SOPs are stored in the Azure Security, Privacy & Compliance SharePoint site. This SharePoint site is accessible to all Azure personnel.  Service teams may supplement the Azure policies and procedures with offering-specific policies and procedures. Service-team-specific policies and procedures associated with identification and authentication are documented and stored within internal Azure SharePoint sites. Only personnel with authorized credentials, adequate levels of permission, legitimate need to know, and specific roles and responsibilities are given access to the service-team-specific policies or procedures. |
| **Part A2**  **Customer Responsibility**  The customer is responsible for procedures to facilitate the implementation of the identification and authentication policy and the associated identification and authentication controls.  **Azure**  The Azure Access Control Standard Operating Procedure (SOP) and the Azure Cryptographic Controls SOP implement the identification and authentication policy and associated controls and documents the following procedures:  \* Identifier management  \* Authenticator management  \* User identification and authentication  \* User authorization  \* Device identification and authentication  \* Key management  Service teams may supplement the Azure policies and procedures with offering-specific policies and procedures. Service-team-specific policies and procedures associated with identification and authentication are documented and stored within internal Azure SharePoint sites. Only personnel with authorized credentials, adequate levels of permission, legitimate need to know, and specific roles and responsibilities are given access to the service-team-specific policies or procedures. |
| **Part B**  **Customer Responsibility**  The customer is responsible for designating an official to manage the development, documentation, and dissemination of the identification and authentication policy and procedures.  **Azure**  The Microsoft Information Risk Management Council (IRMC) organization is the governance body with approval responsibility for the Microsoft Security Policy (MSP) and Microsoft Security Program Policy (MSPP). The IRMC consists of representatives from security and risk management teams across Microsoft including Core Services Engineering and Operations (CSEO), Azure, and Global Security. The Customer Security and Trust: Security Engineering (CST-SE) organization manages the review and approval process and maintains the policies.  On an annual basis, the CST-SE conducts a line-by-line review of the MSP and MSPP. The Microsoft Security Policy (MSP) and Microsoft Security Program Policy (MSPP) Governance document describes each member’s role, types and frequency of review, escalation paths, approval process, and formal publishing procedures of the security policy. Throughout the year, if necessary, CST-SE may convene with the IRMC to conduct reviews after a significant review or change request. The approved policy update is published within the relevant tool on the Microsoft intranet. If service teams establish service-specific or team-specific policies, the respective service teams update the necessary policies at least annually. |
| **Part C1**  **Customer Responsibility**  The customer is responsible for reviewing and updating the current identification and authentication policy on a regular basis and following organization defined events.  **Azure**  The Azure team updates the Azure SOPs at least annually through a formal review process. If needed, the Azure team updates the SOP after a significant change affecting policy execution as well. If established, service-team-specific procedures are updated by their respective teams. The individual service teams review and update their respective SOPs at least annually and when required by a significant change. |
| **Part C2**  **Customer Responsibility**  The customer is responsible for reviewing and updating the identification and authentication procedures on a regular basis and following organization defined events.  **Azure**  The Azure team updates the Azure SOPs at least annually through a formal review process. If needed, the Azure team updates the SOP after a significant change affecting policy execution as well. If established, service-team-specific procedures are updated by their respective teams. The individual service teams review and update their respective SOPs at least annually and when required by a significant change. |

## IA-2 Identification and Authentication (Organizational Users)

Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.

Requirement: For all control enhancements that specify multifactor authentication, the implementation must adhere to the Digital Identity Guidelines specified in NIST Special Publication 800-63B.

Requirement: Multi-factor authentication must be phishing-resistant.

Requirement: All uses of encrypted virtual private networks must meet all applicable Federal requirements and architecture, dataflow, and security and privacy controls must be documented, assessed, and authorized to operate.

Guidance: \"Phishing-resistant\" authentication refers to authentication processes designed to detect and prevent disclosure of authentication secrets and outputs to a website or application masquerading as a legitimate system.

|  |
| --- |
| **IA-2 Control Summary Information** |
| Responsible Roles: OneIdentity, Microsoft Entra ID (formerly AAD), Networking, VPN, Jumpbox |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **IA-2 What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for uniquely identifying and authenticating organizational users.  **Azure**  Azure uniquely identifies and authenticates users via Active Directory (AD), smart cards, or YubiKeys. AD associates users to IDs and GUIDs and prevents the creation of a duplicate account. A user's account within each Azure domain maps his or her Microsoft corporate network (CorpNet) identifier, known as an alias, to the Azure domain for identification and authentication.  Azure utilizes the Global Management Environment (GME), Azure Management Environment (AME), and Public Management Environment (PME) domains for access to the Azure environment. Each domain is specific to the environment.  As an example, John Doe's alias is jdoe, with accounts jdoe@redmond.gbl for access to CorpNet and jdoe@ame.gbl for access to Azure Commercial.  Jumpboxes, Debug servers, Network Hop Boxes, and the SSL VPN are the approved mechanisms by which to gain access to Azure assets via internal network connectivity from CorpNet. A user authenticates to the Jumpbox, Debug server, Network Hop Box, or the SSL VPN with his or her smart card and PIN, then authenticates to the destination asset, with an approved JIT request necessary for elevated access. |

### IA-2(1) - Multi-factor Authentication to Privileged Accounts

Implement multi-factor authentication for access to privileged accounts.

Requirement: According to SP 800-63-3, SP 800-63A (IAL), SP 800-63B (AAL), and SP 800-63C (FAL).

Requirement: Multi-factor authentication must be phishing-resistant.

Guidance: Multi-factor authentication to subsequent components in the same user domain is not required.

|  |
| --- |
| **IA-2(1) Control Summary Information** |
| Responsible Roles: OneIdentity, VPN, Jumpbox |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **IA-2(1) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for implementing multifactor authentication for access to privileged accounts.  **Azure**  Azure uses multifactor authentication for access by Azure personnel using eAuth Level 3 and Federal Information Processing Standards (FIPS) 140-2 and FIPS 140-3 tested Thales Idemia smart cards and Yubico Yubikeys. |

### IA-2(2) - Multi-factor Authentication to Non-privileged Accounts

Implement multi-factor authentication for access to non-privileged accounts.

Requirement: According to SP 800-63-3, SP 800-63A (IAL), SP 800-63B (AAL), and SP 800-63C (FAL).

Requirement: Multi-factor authentication must be phishing-resistant.

Guidance: Multi-factor authentication to subsequent components in the same user domain is not required.

|  |
| --- |
| **IA-2(2) Control Summary Information** |
| Responsible Roles: OneIdentity, VPN, Jumpbox |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **IA-2(2) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for implementing multifactor authentication for access to non-privileged accounts.  **Azure**  Azure uses multifactor authentication for access by Azure personnel using eAuth Level 3 and Federal Information Processing Standards (FIPS) 140-2 and FIPS 140-3 tested Thales Idemia smart cards and Yubico Yubikeys |

### IA-2(5) - Individual Authentication with Group Authentication

When shared accounts or authenticators are employed, require users to be individually authenticated before granting access to the shared accounts or resources.

|  |
| --- |
| **IA-2(5) Control Summary Information** |
| Responsible Roles: OneIdentity, Secret Management Stores, Networking |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☒ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☒ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **IA-2(5) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for requiring individuals using group authenticators to first authenticate using individual authenticators.  **Azure**  Group or shared accounts are not utilized within Azure unless necessary, such as where the local account or accounts cannot be deleted or disabled. For accounts tracked as approved exceptions, the credentials for these accounts are stored in an approved secret management store, which tracks and monitors access to secrets and ensures group or shared account usage is uniquely attributable to the user accessing it by associated the secret store logs with the group or shared account usage. When a user accesses the credentials in the secret management store, that user is identified uniquely, ensuring non-repudiation and attributing user activity to the shared account. |

### IA-2(6) - Access to Accounts -separate Device

Implement multi-factor authentication for [Selection (OneOrMore): local;network;remote] access to [Selection (OneOrMore): privileged accounts;non-privileged accounts] such that:

(a) One of the factors is provided by a device separate from the system gaining access; and

(b) The device meets [FIPS-validated or NSA-approved cryptography].

Guidance: PIV=separate device. Please refer to NIST SP 800-157 Guidelines for Derived Personal Identity Verification (PIV) Credentials.

Guidance: See SC-13 Guidance for more information on FIPS-validated or NSA-approved cryptography.

|  |
| --- |
| **IA-2(6) Control Summary Information** |
| Responsible Roles: OneIdentity, Microsoft Entra ID (formerly AAD), VPN, Jumpbox, Compute |
| Parameter ia-02.06\_odp.01: local, network and remote |
| Parameter ia-02.06\_odp.02: privileged accounts; non-privileged accounts |
| Parameter ia-02.06\_odp.03: FIPS-validated or NSA-approved cryptography |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **IA-2(6) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for implementing multifactor authentication for access to accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets defined strength of mechanism requirements.  **Azure**  Azure implements multifactor authentication for access to privileged and non-privileged accounts through the use of Thales and Idemia smart cards and Yubico Yubikeys. Access requires the user to present a certificate bound to the card or key along with a PIN. |

### IA-2(8) - Access to Accounts - Replay Resistant

Implement replay-resistant authentication mechanisms for access to [Selection (OneOrMore): privileged accounts;non-privileged accounts] .

|  |
| --- |
| **IA-2(8) Control Summary Information** |
| Responsible Roles: Microsoft Entra ID (formerly AAD), Smart Card |
| Parameter ia-02.08\_odp: privileged accounts; non-privileged accounts |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **IA-2(8) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for implementing replay-resistant authentication mechanisms for access to privileged and/or non-privileged accounts.  **Azure**  Azure implements multifactor authentication for network access by Azure personnel with eAuth Level 4 and Federal Information Processing Standards (FIPS) 140-2 compliant Thales smart cards. All Microsoft users connect to Azure assets via Jumpboxes, Debug servers, and Network Hop Boxes. This requires the user to present a certificate bound to the card along with a PIN.  Access to the Azure production environment using the smart card solution is protected from replay attacks by the built-in Kerberos v5 functionality of Active Directory (AD). In Kerberos authentication, the authenticator sent by the client contains additional data, such as an encrypted IP list, the client's timestamp, and the ticket lifetime. If a packet is replayed, the timestamp is checked. If the timestamp is earlier than or the same as a previous authenticator, the packet is rejected because it is a replay.  For more information on Active Directory and Kerberos, see TechNet article 742516: <https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/bb742516(v=technet.10)>  Techniques used to address replay attacks from network connections to the Azure environment include the use of the TLS 1.2/1.3 or higher protocol that uses challenges. The TLS 1.2/1.3 or higher protocol is used to authenticate network access to prove the identities of parties engaged in secure communication. It also provides data integrity through an integrity check value. In addition to protecting against data disclosure, the TLS 1.2/1.3 or higher security protocol can be used to help protect against masquerade attacks, person-in-the-middle or bucket brigade attacks, rollback attacks, and replay attacks. |

### IA-2(12) - Acceptance of PIV Credentials

Accept and electronically verify Personal Identity Verification-compliant credentials.

Guidance: Include Common Access Card (CAC), i.e., the DoD technical implementation of PIV/FIPS 201/HSPD-12.

|  |
| --- |
| **IA-2(12) Control Summary Information** |
| Responsible Roles: Azure Compliance |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☒ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☒ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **IA-2(12) What is the solution and how is it implemented?** |
| **Customer Responsibility**  Government customers using ADFS are responsible for accepting and electronically verifying Personal Identity Verification (PIV) credentials for government customer users. Azure supports the use of PIV and CAC credentials through the use of federated/hybrid identity configured by customers. A customer managed identity provider, such as Active Directory Federation Services (ADFS), is required to support these credential types. See Hybrid Identity Common Scenarios and Recommendations located here <https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-hybrid-identity#common-scenarios-and-recommendations.>  **Azure**  Azure does not utilize Personal Identity Verification (PIV) credentials for internal personnel because PIV cards are not available to Azure.  Azure uniquely identifies and authenticates users via Active Directory (AD), smart cards, or YubiKeys. AD associates users with IDs and GUIDs and prevents the creation of a duplicate account. A user's account within each Azure domain maps his or her Microsoft corporate network (CorpNet) identifier, known as an alias, to the Azure domain for identification and authentication. Azure utilizes the Global Management Environment (GME), Azure Management Environment (AME), and Public Management Environment (PME) domains for access to the Azure environment. Each domain is specific to the environment.  As an example, John Doe's alias is jdoe, with accounts jdoe@redmond.gbl for access to CorpNet and jdoe@ame.gbl for access to Azure Commercial.  Jumpboxes, Debug servers, Network Hop Boxes, and the SSL VPN are the approved mechanisms by which to gain access to Azure assets via internal network connectivity from CorpNet. A user authenticates to the Jumpbox, Debug server, Network Hop Box, or the SSL VPN with his or her smart card and PIN, then authenticates to the destination asset, with an approved JIT request necessary for elevated access. |

## IA-3 Device Identification and Authentication

Uniquely identify and authenticate [devices and/or types of devices to be uniquely identified and authenticated before establishing a connection are defined;] before establishing a [Selection (OneOrMore): local;remote;network] connection.

|  |
| --- |
| **IA-3 Control Summary Information** |
| Responsible Roles: Logging and Monitoring, Networking, Asset Management, Compute |
| Parameter ia-03\_odp.01: all devices within the Azure authorization boundary |
| Parameter ia-03\_odp.02: network |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **IA-3 What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for implementing device identification and authentication prior to establishing a connection.  **Azure**  Azure identifies and authenticates network devices and servers, both physical and virtual.  **Servers**  All Azure physical server name resolution is performed through DNS addresses. Subnets used for the physical server environment use IP addresses provisioned from RFC 1918 non-publicly routable address space. Physical servers are identified and tracked using Datacenter Manager (DCM).  When establishing an Azure subscription, a subscription ID is created. The Fabric Controller (FC), which manages all VMs in Azure, uses this subscription ID to tie VMs to specific subscriptions.  Devices on the Azure environment authenticate with unique identifiers in the form of static MAC addresses and certificates. A physical asset or VM obtains an IP address over the network when it initially boots-up. The Fabric DHCP Server is responsible for assigning IP addresses to physical assets and VMs as determined by the Fabric Controller. This allows the Fabric Controller to take control of managing the IP address pools for the set of physical assets. IPFilter on the operating system (RDOS) is programmed via the Fabric to only allow traffic from specific MAC addresses and specific DIPs, to counter ARP spoofing.  **Network Devices**  As part of the network discovery and configuration steps in the bootstrap workflow, network devices are pre-configured to use DHCP/PXE boot for their configuration. Upon boot of the network device, the bootstrap agent provides the OS image for the device and the basic configuration, including the IP address and credentials, before establishing the connection to the environment. |

## IA-4 Identifier Management

Manage system identifiers by:

a. Receiving authorization from [at a minimum, the ISSO (or similar role within the organization)] to assign an individual, group, role, service, or device identifier;

b. Selecting an identifier that identifies an individual, group, role, service, or device;

c. Assigning the identifier to the intended individual, group, role, service, or device; and

d. Preventing reuse of identifiers for [at least two (2) years].

|  |
| --- |
| **IA-4 Control Summary Information** |
| Responsible Roles: OneIdentity |
| Parameter ia-04\_odp.01: at a minimum, the ISSO (or similar role within the organization) |
| Parameter ia-04\_odp.02: at least two (2) years |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **IA-4 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  The customer is responsible for managing identifiers (i.e., individuals, groups, roles, and devices) for customer resources by receiving authorization from customer-defined personnel/roles prior to assigning identifiers.  **Customer Identity Federation**  Agency customers create their user accounts via the Azure Management Portal. The portal is the entry point for all Azure subscribers. Accounts are automatically created when the service is subscribed. Azure Management Portal user identifiers are defined by the customer. The customer agency is responsible for obtaining authorization from agency organizational officials for access by agency users and ensuring the correct identifier is assigned to the correct agency employee for access to Azure via the Azure Management Portal and agency enablers.  **Azure**  Microsoft implements the identifier management control through the effective use of the corporate network (CorpNet) AD-based user authorization procedures. Microsoft establishes unique identifiers for each user through unique user IDs, based on HR personnel ID numbers. These CorpNet identifiers, known as aliases, are distributed to all Microsoft personnel during the initial CorpNet account creation process.  For personnel supporting Azure services, a user account within each Azure domain ties to the user's CorpNet account using his or her unique CorpNet alias. This alias is consistent across all a user's accounts in all Microsoft domains, including Azure. CorpNet and Azure access are provisioned and managed using separate account management tools. Azure utilizes OneIdentity for both identifier and security group management.  Azure utilizes the Global Management Environment (GME) and Azure Management Environment (AME) domains for access to the Azure environment. Each domain is specific to the environment.  As an example, John Doe's alias is jdoe, with accounts jdoe@redmond.gbl for access to CorpNet and jdoe@ame.gbl for access to Azure Commercial.  Device identifiers are authorized by service team users when adding new devices to the network, consistent with configuration management and inventory management procedures. |
| **Part B**  **Customer Responsibility**  The customer is responsible for selecting identifiers (i.e., individuals, groups, roles, and devices) for customer resources. Customers using identity federation are responsible for selecting and assigning federal/customer user identifiers through their Active Directory management structure which will carry over to Microsoft Entra ID (formerly AAD) through the ADFS Federation. These authentication requests include a claims-based response with group access allowing the unique user to be mapped to the directory synchronized copy of the user in Microsoft Entra ID (formerly AAD).  **Customer Identity Federation**  Customers using identity federation are responsible for selecting and assigning federal/customer user identifiers through their Active Directory management structure which carries over to Microsoft Entra ID (formerly AAD) through the ADFS Federation. These authentication requests include a claims-based response with group access allowing the unique user to be mapped to the directory synchronized copy of the user in Microsoft Entra ID (formerly AAD).  **Azure**  Azure identifies users using the account identifier derived from their Microsoft CorpNet alias as described above. These unique identifiers are not reused for two (2) years.  Device identifiers are selected by service team users when adding new devices to the network, consistent with configuration management and inventory management procedures.  Active Directory is the central account repository used to provide access. |
| **Part C**  **Customer Responsibility**  The customer is responsible for assigning identifiers (i.e., individuals, groups, roles, and devices) for customer resources. Customers using identity federation are responsible for selecting and assigning federal/customer user identifiers through their Active Directory management structure which will carry over to Microsoft Entra ID (formerly AAD) through the ADFS Federation. These authentication requests include a claims-based response with group access allowing the unique user to be mapped to the directory synchronized copy of the user in Microsoft Entra ID (formerly AAD).  **Customer Identity Federation**  Customers using identity federation are responsible for selecting and assigning federal/customer user identifiers through their Active Directory management structure which carries over to Microsoft Entra ID (formerly AAD) through the ADFS Federation. These authentication requests include a claims-based response with group access allowing the unique user to be mapped to the directory synchronized copy of the user in Microsoft Entra ID (formerly AAD).  **Azure**  Active Directory (AD) is the central account repository used to provide access to the service environment.  The Human Resource database is the authoritative source for determining employment status for these AD accounts, as well as establishing the account display name or alias. When the account is created in AD, the unique identifier is created and assigned to the individual.  When adding new devices to the network, service team users assign device identifiers consistent with configuration management and inventory management procedures. |
| **Part D**  **Customer Responsibility**  The customer is responsible for preventing identifier reuse for the customer-defined time period.  **Azure**  Unique user and service or device identifiers are not reused for two (2) years. This is enforced by Active Directory (AD). For users, smart cards are device-unique token identifiers which are uniquely paired to individuals. Smart card certificates are paired to an individual's AD Security Identifier (SID). These unique account identifier and device pairs are not reused. |

### IA-4(4) - Identify User Status

Manage individual identifiers by uniquely identifying each individual as [contractors; foreign nationals].

|  |
| --- |
| **IA-4(4) Control Summary Information** |
| Responsible Roles: OneIdentity |
| Parameter ia-04.04\_odp: contractors; foreign nationals |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☒ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **IA-4(4) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for identifying the status (e.g., contractor, foreign national) of individual users with unique identifiers.  **Azure**  The status of all Microsoft personnel is recorded in OneIdentity, which is the authoritative system for controlling and authorizing account permissions within Azure. Additionally, contractors and vendors are denoted by a prefix, "a-," "b-," or "v-", respectively, associated with their unique AD credentials. Foreign nationals are not uniquely identified in this system as it is a multi-tenant system supporting commercial clients as well as government agencies. Microsoft maintains an operational requirement for this implementation. |

## IA-5 Authenticator Management

Manage system authenticators by:

a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator;

b. Establishing initial authenticator content for any authenticators issued by the organization;

c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;

d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators;

e. Changing default authenticators prior to first use;

f. Changing or refreshing authenticators [a time period for changing or refreshing authenticators by authenticator type is defined;] or when [events that trigger the change or refreshment of authenticators are defined;] occur;

g. Protecting authenticator content from unauthorized disclosure and modification;

h. Requiring individuals to take, and having devices implement, specific controls to protect authenticators; and

i. Changing authenticators for group or role accounts when membership to those accounts changes.

Requirement: Authenticators must be compliant with NIST SP 800-63-3 Digital Identity Guidelines IAL, AAL, FAL level 3. Link https://pages.nist.gov/800-63-3

Guidance: SP 800-63C Section 6.2.3 Encrypted Assertion requires that authentication assertions be encrypted when passed through third parties, such as a browser. For example, a SAML assertion can be encrypted using XML-Encryption, or an OpenID Connect ID Token can be encrypted using JSON Web Encryption (JWE).

|  |
| --- |
| **IA-5 Control Summary Information** |
| Responsible Roles: OneIdentity, Microsoft Entra ID (formerly AAD), Networking |
| Parameter ia-05\_odp.01: seventy (70) days |
| Parameter ia-05\_odp.02: organization-defined events |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **IA-5 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  The customer is responsible for federal/customer user authenticator management and content.  **Azure**  For personnel supporting Azure services, user accounts within Azure domains tie to accounts of existing Microsoft personnel using their unique Microsoft CorpNet aliases. CorpNet and Azure access are provisioned and managed using separate account management tools. CorpNet account management, using MyAccess or CoreIdentity, cannot provide access to Azure – it can only provide access to AD security groups that the Azure account management tool, OneIdentity, leverages. The alias is consistent across all of a user's accounts.  Azure utilizes the AME and GME domains for access to the Azure environment. These domains are specific to the environment.  The identities of accounts are verified during the account request process, where initial authenticator distribution information for new Azure domain accounts are sent to the user's CorpNet e-mail address. Initial authenticator distribution is only sent to the CorpNet e-mail account associated to the provisioning request, after manager approval has been received. Azure-issued smart cards are distributed in person by the C+AI Security smart card support team after confirming the identity of the individual receiving the smart card. |
| **Part B**  **Customer Responsibility**  The customer is responsible for federal/customer user authenticator content.  **Azure**  At the time of initial account creation, Active Directory assigns a unique identification and random temporary password which meets Microsoft Corporate and Azure policy requirements. Active Directory maintains the unique identification associated with the account throughout the life of the account. Account identification is never repeated within Active Directory.  After receiving account creation approval from his/her manager, a new user receives an email from MyAccess or CoreIdentity regarding her or his request. This email has a URL pointer to a uniquely generated page to get a temporary password. This password is randomly generated and may be reset after one (1) day. The initial password generated is in accordance with Identity Management Baseline requirements including complexity and length requirements. After the smart card has been provided to the user, the C+AI Security Smart Card support staff sends IcM tickets for the smart card that needs to be reset. Certain domains are passwordless - the smart card PIN is the authentication method for the account. |
| **Part C**  **Customer Responsibility**  The customer is responsible for federal/customer user authenticator content and password strength.  **Azure**  Issued passwords meet Microsoft Corporate and Azure policy requirements respectively for password complexity. Initial Smart Card certificates are generated by Core Services Engineering and Operations (CSEO). Azure implements a minimum password length of at least fifteen (15) characters and complexity of at least one (1) uppercase, one (1) lowercase, one (1) number, one (1) special character, and passwords may not contain the user's Account Name value or entire Full Name value in accordance with C+AI Security policy. Smart cards are FIPS-140-2 level 3 validated to ensure sufficient strength of hardware token. PINs are required to be at least six characters. |
| **Part D**  **Customer Responsibility**  The customer is responsible for federal/customer user authenticator management and content.  **Azure**  Initial authenticator distribution procedures are noted above. If an authenticator is lost or compromised, Azure administrators reset, re-issue, or revoke the authenticator as needed. |
| **Part E**  **Customer Responsibility**  The customer is responsible for managing their authenticators, including changing default content of authenticators prior to deployment.  **Azure**  Default authentication credentials are often well known, easily discoverable, and present a significant security risk. Therefore, they are changed upon installation. The local administrator account is renamed and disabled. Default passwords are changed for the local administrator account and root accounts for network devices (including SNMP community strings). |
| **Part F**  **Customer Responsibility**  The customer is responsible for managing their authenticators, including changing and refreshing authenticators, and the corresponding time period after which an update is required for each authenticator type.  **Azure**  Passwords must be changed every seventy (70) days. This is defined within the Identity Management Baseline. This is enforced through Microsoft Entra ID (formerly AAD) domain policy settings. Azure considers the incremental risk between 70-day password resets and 60-day password reset values to be minimal.  Azure implements strong password complexity, password expiration, password history, account lockout, and minimum password length per Microsoft Security Standards. Additionally, the use of multifactor authentication further provides strong security controls against credential guessing attacks. Azure considers these mitigating factors sufficient to address the incremental risk between Azure and the required values for password expiration.  For smart cards, PINs are required to be at least six digits. PINs do not currently have maximum lifetimes. |
| **Part G**  **Customer Responsibility**  The customer is responsible for managing and protecting their authenticator content from unauthorized disclosure and modification.  **Azure**  Azure utilizes obscuring mechanisms to protect authenticator content in accordance with the Active Directory settings, specifically the use of encryption to protect authenticator information for encryption and storage. This includes maintaining possession of individual authenticators, not loaning or sharing authenticators with others, and reporting lost or compromised authenticators immediately. |
| **Part H**  **Customer Responsibility**  The customer is responsible for managing their authenticators, including requiring individuals to take, and devices to implement, specific security safeguards to protect authenticators.  **Azure**  Per the Microsoft Security Program Policy (MSPP), authenticators must not be shared or revealed to anyone other than the authorized user. Additionally, authenticators must be promptly changed if they are suspected of being known by unauthorized individuals. Authenticators must not be written down or stored in readable form batch files, automatic log-in scripts, software macros, terminal function keys, in computers without access control, or in other locations where unauthorized persons might discover them and must be masked or encrypted both in storage and transmission. For devices, Azure deploys security controls of credential scanning software to review Microsoft source code for unencrypted credentials and implements Azure Storage automatic encryption for data at rest and HTTPS/TLS 1.2/TLS 1.3 everywhere for data in transit. |
| **Part I**  **Customer Responsibility**  The customer is responsible for managing and changing their authenticators for group and role accounts when membership changes occur.  **Azure**  Group or shared accounts are not utilized within Azure unless necessary, such as where the local account or accounts cannot be deleted or disabled, or where necessary for Break-Glass access. For accounts tracked as approved exceptions, the credentials for these accounts are stored in an approved secret management store, which tracks and monitors access to secrets and ensures group or shared account usage is uniquely attributable to the user accessing it by associated the secret store logs with the group or shared account usage. When a user accesses the credentials in the secret management store, that user is identified uniquely, ensuring non-repudiation and attributing user activity to the shared account.  The approved secret management store enforces rotation of group account credentials every 70 days. Group account credentials are also rotated as needed when group membership changes. |

### IA-5(1) - Password-based Authentication

For password-based authentication:

(a) Maintain a list of commonly-used, expected, or compromised passwords and update the list [the frequency at which to update the list of commonly used, expected, or compromised passwords is defined;] and when organizational passwords are suspected to have been compromised directly or indirectly;

(b) Verify, when users create or update passwords, that the passwords are not found on the list of commonly-used, expected, or compromised passwords in IA-5(1)(a);

(c) Transmit passwords only over cryptographically-protected channels;

(d) Store passwords using an approved salted key derivation function, preferably using a keyed hash;

(e) Require immediate selection of a new password upon account recovery;

(f) Allow user selection of long passwords and passphrases, including spaces and all printable characters;

(g) Employ automated tools to assist the user in selecting strong password authenticators; and

(h) Enforce the following composition and complexity rules: [authenticator composition and complexity rules are defined;].

Requirement: Password policies must be compliant with NIST SP 800-63B for all memorized, lookup, out-of-band, or One-Time-Passwords (OTP). Password policies shall not enforce special character or minimum password rotation requirements for memorized secrets of users.

(h) Requirement: For cases where technology doesn't allow multi-factor authentication, these rules should be enforced: must have a minimum length of 14 characters and must support all printable ASCII characters. For emergency use accounts, these rules should be enforced: must have a minimum length of 14 characters, must support all printable ASCII characters, and passwords must be changed if used.

Guidance: Note that (c) and (d) require the use of cryptography which must be compliant with Federal requirements and utilize FIPS validated or NSA approved cryptography (see SC-13).

|  |
| --- |
| **IA-5(1) Control Summary Information** |
| Responsible Roles: OneIdentity, Microsoft Entra ID (formerly AAD) |
| Parameter ia-05.01\_odp.01: organization-defined frequency |
| Parameter ia-05.01\_odp.02: organization-defined composition and complexity rules |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **IA-5(1) What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  The customer is responsible for maintaining a list of commonly-used, expected, or compromised passwords and updating the list regularly and when organizational passwords are suspected to have been compromised directly or indirectly.  **Azure**  The Azure AD Identity Protection team constantly analyzes Azure AD security telemetry data looking for commonly used weak or compromised passwords. Specifically, the analysis looks for base terms that often are used as the basis for weak passwords. When weak terms are found, they're added to the global banned password list. The contents of the global banned password list aren't based on any external data source, but on the results of Azure AD security telemetry and analysis. |
| **Part B**  **Customer Responsibility**  The customer is responsible for verifying, when created or updated, that the passwords are not found on the list of commonly-used, expected, or compromised passwords in IA-5(1)(a).  **Azure**  When a password is changed or reset for any user in an Azure AD tenant, the current version of the global banned password list is used to validate the strength of the password. This validation check results in stronger passwords for all Azure AD customers. |
| **Part C**  **Customer Responsibility**  The customer is responsible for ensuring passwords are transmitted only over cryptographically-protected channels.  **Azure**  Where passwords exist, Azure applies cryptographic protection to all password in transit. This is a built-in function of Active Directory. Azure leverages HTTPS and TLS 1.2/1.3 protocols for data in transit encryptions. |
| **Part D**  **Customer Responsibility**  The customer is responsible for ensuring passwords are stored using approved cryptographic protections.  **Azure**  Where passwords exist, Azure applies cryptographic protection to all passwords in transmission. This is a built-in function of Active Directory. |
| **Part E**  **Customer Responsibility**  The customer is responsible for requiring immediate selection of a new password upon account recovery.  **Azure**  Where passwords exist, during account creation and recovery, the user is provided with a randomly generated password that must be changed upon initial login. |
| **Part F**  **Customer Responsibility**  The customer is responsible for allowing user selection of long passwords and passphrases, including spaces and all printable characters on customer deployed resources.  **Azure**  Where passwords exist, Active Directory allows passwords and passphrases up to 128 characters in length, and allows the entire set of 95 printable ASCII characters. |
| **Part G**  **Customer Responsibility**  The customer is responsible for employing automated tools to assist the user in selecting strong password authenticators on customer deployed resources.  **Azure**  Where passwords are used, Azure uses Active Directory to determine if password authenticators are sufficiently strong to satisfy the password length, complexity, rotation and lifetime restrictions. Active Directory ensures that the password authenticator strength at creation is sufficient. |
| **Part H**  **Customer Responsibility**  The customer is responsible for enforcing password composition and complexity rules on customer deployed resources.  **Azure**  Azure requires multifactor authentication for all access. Exceptions exist for assets or accounts that are unable to support smart card authentication, including local accounts and certain network devices. Where passwords exist, Azure exceeds Microsoft requirements and implements a minimum password length of at least fifteen (15) characters and complexity of at least one (1) uppercase, one (1) lowercase, one (1) number, and one (1) special character in accordance with C+AI Security policy. |

### IA-5(2) - Public Key-based Authentication

(a) For public key-based authentication:

(1) Enforce authorized access to the corresponding private key; and

(2) Map the authenticated identity to the account of the individual or group; and

(b) When public key infrastructure (PKI) is used:

(1) Validate certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information; and

(2) Implement a local cache of revocation data to support path discovery and validation.

|  |
| --- |
| **IA-5(2) Control Summary Information** |
| Responsible Roles: OneIdentity |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **IA-5(2) What is the solution and how is it implemented?** |
| **Part A1**  **Customer Responsibility**  The customer is responsible for employing PKI-based authentication and enforcing authorized access to private keys within customer-deployed resources.  **Azure**  Microsoft protects private keys by enforcing appropriate and authorized access restrictions. |
| **Part A2**  **Customer Responsibility**  The customer is responsible for employing PKI-based authentication with the ability to map each authenticated identity to the account of the corresponding individual or group within customer-deployed resources.  **Azure**  Smart card certificates include user information for the purposes of mapping the smart card identity to the Active Directory account of the card holder. |
| **Part B1**  **Customer Responsibility**  The customer is responsible for employing PKI-based authentication within customer-deployed resources to validate certifications by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information.  It is the responsibility of the user to protect their private key through limited instances of the private key and encryption of the private key.  Azure provides the capability to customers to access their accounts programmatically through the SMAPI that relies on public/private key pairs. It is the customer's responsibility to properly set up and configure the key pairs. It is also the responsibility of the customer to manage private keys and revoke any certificates that have been compromised or expired.  When using the SMAPI interface, authentication does not use the federated identity. Instead, the customer should generate a public/private key pair and self-signed certificate and registers that certificate using the portal. The certificate is then used as a client certificate in the RPC over HTTPS connection to SMAPI. Customer is responsible for protecting private keys generated.  **Azure**  Microsoft’s corporate PKI has been established to provide a variety of digital certificate services to support operations for Azure and for the Microsoft corporation. The Microsoft corporate PKI functions as the Certificate Authority (CA) and Registration Authority (RA) and provides directory services to manage keys and certificates. The certificates are signed by an internal Microsoft CA and are validated against that CA's public key. Azure also checks certificates against certificate revocation lists.  PKI certificates are stored within smart cards and authorized access to the corresponding private keys are enforced. Access to certs is restricted via PIN requirements to gain access to the certificate stored on the card. The Azure PKI intermediate CA servers are members of only internally rooted PKI chains, permitting the issuance of certificates to users and computers within the Azure AD environments. Azure validates the certificates by constructing a certification path with status information to an accepted trust anchor. |
| **Part B2**  **Customer Responsibility**  The customer is responsible for employing PKI-based authentication within customer-deployed resources and implementing a local cache of private key data to support path discovery and validation when unable to access this information via the network.  **Azure**  Azure domain controllers cache revocation data and make it available to Azure assets if the primary revocation lists are unavailable. |

### IA-5(6) - Protection of Authenticators

Protect authenticators commensurate with the security category of the information to which use of the authenticator permits access.

|  |
| --- |
| **IA-5(6) Control Summary Information** |
| Responsible Roles: Azure Security |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **IA-5(6) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer agency is responsible for ensuring their authorized users protect all provided authenticators, including passwords. Customer agency users should protect authenticators with the classification or sensitivity of the information accessed.  **Azure**  All passwords used to access the Microsoft corporate network or business information must be considered and handled as “information as per the InfoSec #2.0 Information Classification and Handling Standard.” Core Services Engineering and Operations (CSEO) is responsible for protecting Microsoft corporate network authenticators.  Per the Identity Management Standard, usernames and passwords are never stored or transmitted in the clear or any unencrypted format. Passwords must not be shared or revealed to anyone other than the authorized user. Additionally, passwords must be promptly changed if they are suspected of being known by unauthorized individuals.  Per Azure policy, cryptographic protection is applied to passwords when transmitted and stored, and are never transmitted in any unencrypted format natively within the Azure environment.  Cryptographic certificates are stored in an approved secret management store. Information stored in the approved secret management stores is encrypted, and access occurs over an encrypted channel.  Authentication credentials, such as username/password pairs, are considered High Business Impact (HBI) data and are required to be protected based upon its classification. Encryption must be used when storing or transmitting passwords, username/password files, or authentication tokens, in accordance with Asset Protection Standard. Azure uses the following authentication protocols with commensurate encryption.  **Kerberos V5**  Kerberos is a network authentication protocol. It is designed to provide strong authentication for client/server applications by using secret-key cryptography. The Kerberos protocol uses strong cryptography so that a client can prove its identity to a server (and vice versa) across an insecure network connection.  The Kerberos V5 protocol can use both symmetric and asymmetric encryption. Because most Kerberos encryption methods are based on keys that can be created only by the KDC and the client, or by the KDC and a network service, the Kerberos V5 protocol is said to use symmetric encryption. That is, the same key is used to encrypt and decrypt messages.  Microsoft’s implementation of the Kerberos protocol can also make limited use of asymmetric encryption. A private/public key pair can be used to encrypt or decrypt initial authentication messages from a network client or a network service as in the case of public key certificates on smart cards.  **NTLMv2**  NTLM credentials are based on data obtained during the interactive logon process and consist of a domain name, a username, and a one-way hash of the user's password. NTLM uses an encrypted challenge/response protocol to authenticate a user without sending the user's password over the wire. Instead, the system requesting authentication must perform a calculation that proves it has access to the secured NTLM credentials.  Interactive NTLM authentication over a network typically involves two systems: a client system, where the user is requesting authentication, and a domain controller, where information related to the user's password is kept. Noninteractive authentication, which may be required to permit an already logged-on user to access a resource such as a server application, typically involves three systems: a client, a server, and a domain controller that does the authentication calculations on behalf of the server.  The following steps present an outline of NTLM noninteractive authentication. The first step provides the user's NTLM credentials and occurs only as part of the interactive authentication (logon) process.  1. (Interactive authentication only) A user accesses a client computer and provides a domain name, username, and password. The client computes a cryptographic hash of the password and discards the actual password.  2. The client sends the username to the server.  3. The server generates a 16-byte random number, called a challenge or nonce, and sends it to the client.  4. The client encrypts this challenge with the hash of the user's password and returns the result to the server. This is called the response.  5. The server sends the following items to the domain controller - username; challenge sent to the client; response received from the client.  6. The domain controller uses the username to retrieve the hash of the user's password from the Security Account Manager database. It uses this password hash to encrypt the challenge.  7. The domain controller compares the encrypted challenge it computed (in step 6) to the response computed by the client (in step 4). If they are identical, authentication is successful. |

### IA-5(7) - No Embedded Unencrypted Static Authenticators

Ensure that unencrypted static authenticators are not embedded in applications or other forms of static storage.

Guidance: In this context, prohibited static storage refers to any storage where unencrypted authenticators, such as passwords, persist beyond the time required to complete the access process.

|  |
| --- |
| **IA-5(7) Control Summary Information** |
| Responsible Roles: SDL |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **IA-5(7) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for ensuring there are no unencrypted static authenticators within customer-deployed resources.  **Azure**  Azure explicitly prohibits the use of unencrypted static authenticators embedded in applications, access scripts, or function keys. Any script that uses an authenticator makes a call to a secrets management database prior to each use. Access to the secrets management database is audited, which allows detection of violations of this prohibition if a service account is used to access a system without a corresponding call to the secrets management database.  Azure service teams perform security testing for Azure services through the Security Development Lifecycle (SDL) process that is followed for all engineering projects. As part of the security testing that occurs during multiple phases of the SDL process, Azure teams ensure there are no unencrypted authenticators embedded in the applications, access scripts or function keys. CredScan is utilized on all official builds in all build pipelines, and either breaking the build process preventing production use or creating work items assigned to the Azure service team for remediation. |

### IA-5(8) - Multiple System Accounts

Implement [different authenticators in different user authentication domains] to manage the risk of compromise due to individuals having accounts on multiple systems.

Guidance: If a single user authentication domain is used to access multiple systems, such as in single-sign-on, then only a single authenticator is required.

|  |
| --- |
| **IA-5(8) Control Summary Information** |
| Responsible Roles: OneIdentity |
| Parameter ia-05.08\_odp: different authenticators in different user authentication domains |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **IA-5(8) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for managing the risk imposed by users with multiple accounts on customer-deployed resources (e.g., having different authenticators on all systems, employing some form of single sign-on mechanism, or including some form of one-time passwords on all systems).  **Azure**  Azure uses smart cards that differentiate between different Microsoft Entra ID (formerly AAD) domains. This ensures that personnel use different authenticators when accessing the two domains and prevents an attacker from gaining access to both domains if one set of authenticators is compromised. In addition, Azure uses single-sign-on, encryption of AAD passwords that exist in the back-end and passwords utilized where smart cards are not possible via storage in Azure Key Vault, and encryption of all traffic with HTTPS, mitigating the risk of compromise. |

### IA-5(13) - Expiration of Cached Authenticators

Prohibit the use of cached authenticators after [the time period after which the use of cached authenticators is prohibited is defined;].

Guidance: For components subject to configuration baseline(s) (such as STIG or CIS,) the time period should conform to the baseline standard.

|  |
| --- |
| **IA-5(13) Control Summary Information** |
| Responsible Roles: Microsoft Entra ID (formerly AAD) |
| Parameter ia-05.13\_odp: time period |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☒ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☒ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **IA-5(13) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for enforcing the expiration of cached authenticators.  **Azure**  Azure does not allow the use of cached authenticators within the Azure environment. Once a session has closed or the user has logged off, the user must re-authenticate to the system. |

## IA-6 Authentication Feedback

Obscure feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals.

|  |
| --- |
| **IA-6 Control Summary Information** |
| Responsible Roles: OneIdentity, Networking, VPN, Jumpbox, Storage |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **IA-6 What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for obscuring authentication feedback information during the authentication process for any customer-deployed resources.  **Azure**  Azure protects authenticator feedback using the built-in operating system security controls that protect passwords when authenticating to system components. Additionally, SSH and Remote Desktop Protocol (RDP) are used for authentication into the Azure production environment and provide obfuscation of credentials. No feedback is provided during the authentication process that could lead to potential exploitation by unauthorized users. Authenticators are displayed as asterisks so that the user is aware an authenticator is being entered, but the authenticator cannot be viewed.  Azure applies cryptographic protection to all secrets in transit and at rest. Azure leverages HTTPS and TLS 1.2/1.3 protocols for data in transit encryptions. Azure Storage automatically encrypts secrets data when persisting it to the cloud. Data in Azure Storage is encrypted and decrypted transparently using 256-bit AES encryption, one of the strongest block ciphers available, and is Federal Information Processing Standards (FIPS) 140-2 tested. |

## IA-7 Cryptographic Module Authentication

Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, executive orders, directives, policies, regulations, standards, and guidelines for such authentication.

|  |
| --- |
| **IA-7 Control Summary Information** |
| Responsible Roles: OneIdentity, Secret Management Stores |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **IA-7 What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for implementing mechanisms for authentication to a cryptographic module (e.g., configuring web applications). Customers are responsible for configuring their web browsers, mobile devices, etc., to enable communications through FIPS 140-2 compliant encryption. Customers who enforce FDCC/USGCB settings on their government computers or enablers (for REST API) will achieve FIPS 140-2 encryption for data transmitted to Azure between their enablers (for REST API) and the Azure Web services interface. Strong encryption with FIPS-approved ciphers is still possible if workstations are not operating in FIPS mode.  Azure SDK extends the core .NET libraries to allow developers to integrate the .NET Cryptographic Service Providers (CSPs) within Azure. Developers familiar with .NET CSPs can easily implement encryption, hashing, and key management functionality for stored or transmitted data.  **Azure**  Azure implements encryption mechanisms on all internal and customer communications using cryptographic certificates issued by Certificate Management Tool which are anchored to the root Certificate Authority (CA). To request a cryptographic certificate, the Azure user interacts with an approved secret management store. The secret management store then interacts with Certificate Management Tool to process the request. The request is routed to the user’s manager for approval. Once the certificate is issued, the user uses multifactor authentication to access Azure assets to install the certificate. This process meets the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module.  Encryption mechanisms and techniques used by Azure follow the requirements and restrictions outlined in the Microsoft Cryptographic Standards for SDL Covered Products. These standards are in line with the use of only Federal Information Processing Standards (FIPS) 140-2 compliant cyphers. Service data and information are handled in accordance with the requirements and restrictions specified in the Asset Classification Standard and the Asset Protection Standard when cryptography is used. The Asset Classification Standard and Asset Protection Standard establish the mandatory minimum requirements for Microsoft’s online services’ asset ownership, classification, and protection. Azure utilizes encryption for user authentication through Active Directory. The following FIPS-approved algorithms are supported:  \* 3651 - Secure Kernel Code Integrity  \* 3644 - Code Integrity  \* 3615 - Windows OS Loader  \* 3527 - Kernel Mode Cryptographic Primitives Library  \* 3513 - Secure Kernel Code Integrity (skci.dll) in Windows 10 Pro, Windows 10 Enterprise, Windows 10 Enterprise LTSB, Windows Server 2016 Standard, Windows Server 2016 Datacenter, Windows Storage Server 2016  \* 3510 - Code Integrity (ci.dll) in Microsoft Windows 10, Windows 10 Pro, Windows 10 Enterprise, Windows 10 Enterprise LTSB, Windows 10 Mobile, Windows Server 2016 Standard, Windows Server 2016 Datacenter, Windows Storage Server 2016  \* 3502 - BitLocker® Windows OS Loader (winload) in Microsoft Windows 10, Windows 10 Pro, Windows 10 Enterprise, Windows 10 Enterprise LTSB, Windows 10 Mobile, Windows Server 2016 Standard, Windows Server 2016 Datacenter, Windows Storage Server 2016  \* 3501 - BitLocker® Windows Resume (winresume) in Microsoft Windows 10, Windows 10 Pro, Windows 10 Enterprise, Windows 10 Enterprise LTSB, Windows Server 2016 Standard, Windows Server 2016 Datacenter, Windows Storage Server 2016  \* 3487 - Boot Manager in Microsoft Windows 10, Windows 10 Pro, Windows 10 Enterprise, Windows 10 Enterprise LTSB, Windows 10 Mobile, Windows Server 2016 Standard, Windows Server 2016 Datacenter, Windows Storage Server 2016  \* 3480 - Windows OS Loader  \* 3690 - Virtual TPM  \* 3197 - Cryptographic Primitives Library  \* 3196 - Kernel Mode Cryptographic Primitives Library  \* 3195 - Code Integrity  \* 3194 - Windows OS Loader  \* 3096 - Secure Kernel Code Integrity  \* 3095 - Cryptographic Primitives Library  \* 3094 - Kernel Mode Cryptographic Primitives Library  \* 3093 - Code Integrity  \* 3092 - BitLocker Dump Filter  \* 3091 - Windows Resume  \* 3090 - Windows OS Loader  \* 3089 - Boot Manager  \* 2938 - Secure Kernel Code Integrity (skci.dll) in Windows 10 Pro, Windows 10 Enterprise, Windows 10 Enterprise LTSB, Windows Server 2016 Standard, Windows Server 2016 Datacenter, Windows Storage Server 2016  \* 2937 - Cryptographic Primitives Library (bcryptprimitives.dll and ncryptsslp.dll) in Microsoft Windows 10, Windows 10 Pro, Windows 10 Enterprise, Windows 10 Enterprise LTSB, Windows 10 Mobile, Windows Server 2016 Standard, Windows Server 2016 Datacenter, Windows Storage Server 2016, Azure Host OS (version 1.65)  \* 2936 - Kernel Mode Cryptographic Primitives Library (cng.sys) in Microsoft Windows 10, Windows 10 Pro, Windows 10 Enterprise, Windows 10 Enterprise LTSB, Windows 10 Mobile, Windows Server 2016 Standard, Windows Server 2016 Datacenter, Windows Storage Server 2016, Azure Host OS (version 1.65)  \* 2935 - Code Integrity (ci.dll) in Microsoft Windows 10, Windows 10 Pro, Windows 10 Enterprise, Windows 10 Enterprise LTSB, Windows 10 Mobile, Windows Server 2016 Standard, Windows Server 2016 Datacenter, Windows Storage Server 2016, Azure Host OS (version 1.65)  \* 2934 - BitLocker® Dump Filter (dumpfve.sys) in Windows 10 Pro, Windows 10 Enterprise, Windows 10 Enterprise LTSB, Windows 10 Mobile, Windows Server 2016 Standard, Windows Server 2016 Datacenter, Windows Storage Server 2016, Azure Host OS (version 1.65)  \* 2933 - BitLocker® Windows Resume (winresume) in Microsoft Windows 10, Windows 10 Pro, Windows 10 Enterprise, Windows 10 Enterprise LTSB, Windows Server 2016 Standard, Windows Server 2016 Datacenter, Windows Storage Server 2016  \* 2932 - BitLocker® Windows OS Loader (winload) in Microsoft Windows 10, Windows 10 Pro, Windows 10 Enterprise, Windows 10 Enterprise LTSB, Windows 10 Mobile, Windows Server 2016 Standard, Windows Server 2016 Datacenter, Windows Storage Server 2016, Azure Host OS (version 1.65)  \* 2931 - Boot Manager in Microsoft Windows 10, Windows 10 Pro, Windows 10 Enterprise, Windows 10 Enterprise LTSB, Windows 10 Mobile, Windows Server 2016 Standard, Windows Server 2016 Datacenter, Windows Storage Server 2016, Azure Host OS (version 1.65)  \* 2357 - Cryptographic Primitives Library (bcryptprimitives.dll and ncryptsslp.dll) in Microsoft Windows 8.1 Enterprise, Windows Server 2012 R2, Windows Storage Server 2012 R2, Surface Pro 3, Surface Pro 2, Surface Pro, Surface 2, Surface, Windows RT 8.1, Windows Phone 8.1, Windows Embedded 8.1 Industry Enterprise, StorSimple 8000 Series, Azure StorSimple Virtual Array Windows Server 2012 R2  \* 2356 - Kernel Mode Cryptographic Primitives Library (cng.sys) in Microsoft Windows 8.1 Enterprise, Windows Server 2012 R2, Windows Storage Server 2012 R2, Surface Pro 3, Surface Pro 2, Surface Pro, Surface 2, Surface, Windows RT 8.1, Windows Phone 8.1, Windows Embedded 8.1 Industry Enterprise, StorSimple 8000 Series, Azure StorSimple Virtual Array Windows Server 2012 R2  \* 2355 - Code Integrity (ci.dll) in Microsoft Windows 8.1 Enterprise, Windows Server 2012 R2, Windows Storage Server 2012 R2, Surface Pro 3, Surface Pro 2, Surface Pro, Surface 2, Surface, Windows RT 8.1, Windows Phone 8.1, Windows Embedded 8.1 Industry Enterprise, StorSimple 8000 Series, Azure StorSimple Virtual Array Windows Server 2012 R2  \* 2354 - BitLocker® Dump Filter (dumpfve.sys) in Microsoft Windows 8.1 Enterprise, Windows Server 2012 R2, Windows Storage Server 2012 R2, Surface Pro 3, Surface Pro 2, Surface Pro,Surface 2, Surface, Windows RT 8.1, Windows Phone 8.1, Windows Embedded 8.1 Industry Enterprise, StorSimple 8000 Series  \* 2353 - BitLocker® Windows Resume (winresume) in Microsoft Windows 8.1 Enterprise, Windows Server 2012 R2, Windows Storage Server 2012 R2, Surface Pro 3, Surface Pro 2, Surface Pro, Windows Embedded 8.1 Industry Enterprise, StorSimple 8000 Series  \* 2352 - BitLocker® Windows OS Loader (winload) in Microsoft Windows 8.1 Enterprise, Windows Server 2012 R2, Windows Storage Server 2012 R2, Surface Pro 3, Surface Pro 2, Surface Pro, Surface 2, Surface, Windows RT 8.1, Windows Phone 8.1, Windows Embedded 8.1 Industry Enterprise, StorSimple 8000 Series, Azure StorSimple Virtual Array Windows Server 2012 R2  \* 2351 - Boot Manager in Microsoft Windows 8.1 Enterprise, Windows Server 2012 R2, Windows Storage Server 2012 R2, Surface Pro 3, Surface Pro 2, Surface Pro, Surface 2, Surface, Windows RT 8.1, Windows Phone 8.1, Windows Embedded 8.1 Industry Enterprise, StorSimple 8000 Series, Azure StorSimple Virtual Array Windows Server 2012 R2  \* 3651 - Secure Kernel Code Integrity  \* 3644 - Code Integrity  \* 3615 - Windows OS Loader  \* 3197 - Cryptographic Primitives Library  \* 3196 - Kernel Mode Cryptographic Primitives Library  \* 3092 - BitLocker Dump Filter  \* 3089 - Boot Manager  **Network Devices**  AES-256 bit encrypted SSH is used for network device authentication using Federal Information Processing Standards (FIPS) 140-2 approved algorithms:  \* 0048 - SecureCRT VanDyke 8.0.3 (FIPS Validation Certificate 0048)  \* 2643 - nShield F2 500+, nShield F2 1500+ and nShield F2 6000+  **Azure Key Stores**  The Thales nShield Hardware Security Modules used by KeyVault employ cryptographic modules certified by NIST as being Federal Information Processing Standards (FIPS) 140-2 compliant; relevant NIST certificate number is 2643. Azure Managed HSM and KeyVault utilize CMVP certificate number 4399 from Marvell vendor. Azure Dedicated HSM utilizes CMVP certificate numbers 4090 and 4684 certificate numbers from Thales vendor. Azure leverages the NIST CMVP certificate numbers 3517, 3914, and 3907 for Yubico, Inc. cryptographic modules to enable multi-factor authentication within Azure cloud production environments. |

## IA-8 Identification and Authentication (Non-organizational Users)

Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users.

|  |
| --- |
| **IA-8 Control Summary Information** |
| Responsible Roles: Azure Compliance |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☒ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☒ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **IA-8 What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for identifying and authenticating non-organizational users accessing customer-deployed resources.  **Azure**  Azure does not allow any non-organizational users to authenticate to internal production services. |

### IA-8(1) - Acceptance of PIV Credentials from Other Agencies

Accept and electronically verify Personal Identity Verification-compliant credentials from other federal agencies.

|  |
| --- |
| **IA-8(1) Control Summary Information** |
| Responsible Roles: Azure Compliance |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☒ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☒ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **IA-8(1) What is the solution and how is it implemented?** |
| **Customer Responsibility**  Government customers using ADFS are responsible for accepting and electronically verifying Personal Identity Verification (PIV) credentials for government customer users. Azure supports the use of PIV and CAC credentials through the use of federated/hybrid identity configured by customers. A customer managed identity provider, such as Active Directory Federation Services (ADFS), is required to support these credential types. See Hybrid Identity Common Scenarios and Recommendations located here <https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-hybrid-identity#common-scenarios-and-recommendations.>  **Azure**  Azure does not allow any non-organizational users to authenticate to internal production services. Azure does not utilize Personal Identity Verification (PIV) credentials for internal personnel because PIV cards are not available to Azure. |

### IA-8(2) - Acceptance of External Authenticators

(a) Accept only external authenticators that are NIST-compliant; and

(b) Document and maintain a list of accepted external authenticators.

|  |
| --- |
| **IA-8(2) Control Summary Information** |
| Responsible Roles: Azure Compliance |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☒ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☒ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **IA-8(2) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for only accepting third-party credentials that have been approved by the Federal Identity, Credential, and Access Management (FICAM) Trust Framework Solutions initiative. Note: if the customer’s deployed resources do not allow third-party credentials this control is not applicable.  **Azure**  Azure does not allow any non-organizational users to authenticate to internal production services. Azure does not accept or process any third-party credentials. |

### IA-8(4) - Use of Defined Profiles

Conform to the following profiles for identity management [identity management profiles are defined;].

|  |
| --- |
| **IA-8(4) Control Summary Information** |
| Responsible Roles: Azure Compliance |
| Parameter ia-08.04\_odp: identity management profiles |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☒ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☒ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **IA-8(4) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for conforming to the profiles issued by the Federal Identity, Credential, and Access Management (FICAM) Trust Framework Solutions initiative. Note: if the customer’s deployed resources do not allow third-party credentials this control is not applicable.  **Azure**  Azure does not allow any non-organizational users to authenticate to internal production services. Azure does not accept or process any third-party credentials. |

## IA-11 Re-authentication

Require users to re-authenticate when [circumstances or situations requiring re-authentication are defined;].

Guidance: The fixed time period cannot exceed the limits set in SP 800-63. At this writing they are: \* AAL3 (high baseline) \* 12 hours or \* 15 minutes of inactivity

|  |
| --- |
| **IA-11 Control Summary Information** |
| Responsible Roles: JIT |
| Parameter ia-11: organization-defined circumstances or situations requiring re-authentication |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **IA-11 What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for requiring users to re-authenticate when organization-defined circumstances or situations require re-authentication.  **Azure**  By default, accounts do not have active elevated permissions to the production environment. Elevation requires a user to request temporary Just In Time (JIT) access through the JIT portal. Azure requires users to re-authenticate when one of two situations occur:  \* When the user's credentials change or authenticators expire, or  \* When privilege escalation is required, such as when JIT access is needed  When authenticators expire, an Azure user must reauthenticate following the password change. When an Azure user require administrative access to services within the environment, they must submit a request for elevation and be granted access via the JIT service. Access via JIT requires the creation of temporary authenticators, requiring an additional level of access control.  Azure leverages Secure Admin Workstation (SAW) workstations which serve as gateway into Azure FedRAMP High and DoD SRG defined authorization boundary. The screensaver session lock is activated within 10 minutes of inactivity on the Secure Admin Workstation (SAW). Therefore, personnel are required to re-authenticate within 10 minutes of inactivity from the SAW workstations. |

## IA-12 Identity Proofing

a. Identity proof users that require accounts for logical access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines;

b. Resolve user identities to a unique individual; and

c. Collect, validate, and verify identity evidence.

Guidance: In accordance with NIST SP 800-63A Enrollment and Identity Proofing

|  |
| --- |
| **IA-12 Control Summary Information** |
| Responsible Roles: OneIdentity, HR, CorpNet |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **IA-12 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  The customer is responsible for identity proofing users that require accounts for logical access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines.  **Azure**  As a part of initial account setup on Microsoft's corporate network, known as CorpNet, all Microsoft personnel have their identity validated using government-issued identification. This identity validation is then used to activate the user's CorpNet account, known as an alias. This alias is then used to implement non-repudiation throughout all Azure production environments. Access to production Azure clouds is requested via the CorpNet alias, ensuring identity proofing is implemented across all clouds. This alias is consistent across all a user's accounts in all Microsoft domains. All Azure access requests and approvals leverage these CorpNet aliases. New Azure user accounts refer to identities of existing Microsoft users using their unique CorpNet identifiers, known as aliases, who require access to Azure resources. The validation is conducted virtually by the third-party vendor, HireRight. Their responsibility is to perform background checks and verify government-issued IDs prior to the issuance of CorpNet aliases to Microsoft personnel. This process ensures the integrity and security of Microsoft Azure operations.  Azure smart cards tied to the specific environment of access are shipped via FedEx in a deactivated state and cannot be used until they are activated. A note is added to the user's account confirming the shipping number for tracking. Shipments require a signature for delivery. Smart cards are not activated until Core Services Engineering and Operations (CSEO) receives a confirmation email from the recipient, recipient's manager, AAM, or Security, ensuring the user's alias is consistent and validating the user's identity. The recipient must email the ticketing team from their Microsoft corporate email. The ticketing team provides the response. The smart card team works with the recipient to unlock their smart card via the ticketing tool. If the user is located in the Puget Sound region, they must come to the main Microsoft campus to pick up their smart card. If the user is outside of the Puget Sound region, the smart card is shipped directly to the individual and auto-disabled until activated by the user. |
| **Part B**  **Customer Responsibility**  The customer is responsible for resolving user identities to a unique individual.  **Azure**  The Microsoft CorpNet alias that follows all Microsoft personnel is unique, and ensures that non-repudiation is implemented and Azure is able to resolve user identities to a unique individual. This CorpNet alias is used in all Azure identity domains to ensure non-repudiation and resolution of user identities to a unique individual globally across all clouds. |
| **Part C**  **Customer Responsibility**  The customer is responsible for collecting, validating, and verifying identity evidence.  **Azure**  As a part of initial account setup on the Microsoft corporate network (CorpNet), all Microsoft personnel have their identity validated using government-issued identification. This establishes the user's alias, which is then used to implement non-repudiation throughout all Azure production environments. Access to production Azure clouds is then requested via the CorpNet alias, ensuring identity proofing is implemented across all clouds. |

### IA-12(2) - Identity Evidence

Require evidence of individual identification be presented to the registration authority.

|  |
| --- |
| **IA-12(2) Control Summary Information** |
| Responsible Roles: OneIdentity, HR, CorpNet |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **IA-12(2) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for requiring evidence of individual identification be presented to the registration authority.  **Azure**  As a part of initial account setup on Microsoft's corporate network, known as CorpNet, all Microsoft personnel have their identity validated using government-issued identification. This identity validation is then used to activate the user's CorpNet account, known as an alias. This alias is then used to implement non-repudiation throughout all Azure production environments. Access to production Azure clouds is requested via the CorpNet alias, ensuring identity proofing is implemented across all clouds. This alias is consistent across all a user's accounts in all Microsoft domains. All Azure access requests and approvals leverage these CorpNet aliases. New Azure user accounts refer to identities of existing Microsoft users using their unique CorpNet identifiers, known as aliases, who require access to Azure resources. The validation is conducted virtually by the third-party vendor, HireRight. Their responsibility is to perform background checks and verify government-issued IDs prior to the issuance of CorpNet aliases to Microsoft personnel. This process ensures the integrity and security of Microsoft Azure operations.  Azure smart cards tied to the specific environment of access are shipped via FedEx in a deactivated state and cannot be used until they are activated. A note is added to the user's account confirming the shipping number for tracking. Shipments require a signature for delivery. Smart cards are not activated until Core Services Engineering and Operations (CSEO) receives a confirmation email from the recipient, recipient's manager, AAM, or Security, ensuring the user's alias is consistent and validating the user's identity. The recipient must email the ticketing team from their Microsoft corporate email. The ticketing team provides the response. The smart card team works with the recipient to unlock their smart card via the ticketing tool. If the user is located in the Puget Sound region, they must come to the main Microsoft campus to pick up their smart card. If the user is outside of the Puget Sound region, the smart card is shipped directly to the individual and auto-disabled until activated by the user. |

### IA-12(3) - Identity Evidence Validation and Verification

Require that the presented identity evidence be validated and verified through [methods of validation and verification of identity evidence are defined;].

|  |
| --- |
| **IA-12(3) Control Summary Information** |
| Responsible Roles: OneIdentity, HR, CorpNet |
| Parameter ia-12.03\_odp: organizational defined methods of validation and verification |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **IA-12(3) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for requiring that the presented identity evidence be validated and verified through organizational defined methods of validation and verification.  **Azure**  As a part of initial account setup on Microsoft's corporate network, known as CorpNet, all Microsoft personnel have their identity validated using government-issued identification. This identity validation is then used to activate the user's CorpNet account, known as an alias. This alias is then used to implement non-repudiation throughout all Azure production environments. Access to production Azure clouds is requested via the CorpNet alias, ensuring identity proofing is implemented across all clouds. This alias is consistent across all a user's accounts in all Microsoft domains. All Azure access requests and approvals leverage these CorpNet aliases. New Azure user accounts refer to identities of existing Microsoft users using their unique CorpNet identifiers, known as aliases, who require access to Azure resources. The validation is conducted virtually by the third-party vendor, HireRight. Their responsibility is to perform background checks and verify government-issued IDs prior to the issuance of CorpNet aliases to Microsoft personnel. This process ensures the integrity and security of Microsoft Azure operations.  Azure smart cards tied to the specific environment of access are shipped via FedEx in a deactivated state and cannot be used until they are activated. A note is added to the user's account confirming the shipping number for tracking. Shipments require a signature for delivery. Smart cards are not activated until Core Services Engineering and Operations (CSEO) receives a confirmation email from the recipient, recipient's manager, AAM, or Security, ensuring the user's alias is consistent and validating the user's identity. The recipient must email the ticketing team from their Microsoft corporate email. The ticketing team provides the response. The smart card team works with the recipient to unlock their smart card via the ticketing tool. If the user is located in the Puget Sound region, they must come to the main Microsoft campus to pick up their smart card. If the user is outside of the Puget Sound region, the smart card is shipped directly to the individual and auto-disabled until activated by the user. |

### IA-12(4) - In-person Validation and Verification

Require that the validation and verification of identity evidence be conducted in person before a designated registration authority.

|  |
| --- |
| **IA-12(4) Control Summary Information** |
| Responsible Roles: OneIdentity, HR, CorpNet |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☒ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **IA-12(4) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for requiring that the validation and verification of identity evidence be conducted in person before a designated registration authority.  **Azure**  As a part of initial account setup on Microsoft's corporate network, known as CorpNet, all Microsoft personnel have their identity validated using government-issued identification. This identity validation is then used to activate the user's CorpNet account, known as an alias. This alias is then used to implement non-repudiation throughout all Azure production environments. Access to production Azure clouds is requested via the CorpNet alias, ensuring identity proofing is implemented across all clouds. This alias is consistent across all a user's accounts in all Microsoft domains. All Azure access requests and approvals leverage these CorpNet aliases. New Azure user accounts refer to identities of existing Microsoft users using their unique CorpNet identifiers, known as aliases, who require access to Azure resources. The validation is conducted virtually by the third-party vendor, HireRight. Their responsibility is to perform background checks and verify government-issued IDs prior to the issuance of CorpNet aliases to Microsoft personnel. This process ensures the integrity and security of Microsoft Azure operations.  Azure smart cards tied to the specific environment of access are shipped via FedEx in a deactivated state and cannot be used until they are activated. A note is added to the user's account confirming the shipping number for tracking. Shipments require a signature for delivery. Smart cards are not activated until Core Services Engineering and Operations (CSEO) receives a confirmation email from the recipient, recipient's manager, AAM, or Security, ensuring the user's alias is consistent and validating the user's identity. The recipient must email the ticketing team from their Microsoft corporate email. The ticketing team provides the response. The smart card team works with the recipient to unlock their smart card via the ticketing tool. If the user is located in the Puget Sound region, they must come to the main Microsoft campus to pick up their smart card. If the user is outside of the Puget Sound region, the smart card is shipped directly to the individual and auto-disabled until activated by the user. |

### IA-12(5) - Address Confirmation

Require that a [Selection: registration code;notice of proofing] be delivered through an out-of-band channel to verify the users address (physical or digital) of record.

Guidance: In accordance with NIST SP 800-63A Enrollment and Identity Proofing

|  |
| --- |
| **IA-12(5) Control Summary Information** |
| Responsible Roles: OneIdentity, HR, CorpNet |
| Parameter ia-12.05\_odp: Azure smart card |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **IA-12(5) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for requiring that a registration code or notice of proofing be delivered through an out-of-band channel to verify the users address (physical or digital) of record.  **Azure**  As a part of initial account setup on Microsoft's corporate network, known as CorpNet, all Microsoft personnel have their identity validated using government-issued identification. This identity validation is then used to activate the user's CorpNet account, known as an alias. This alias is then used to implement non-repudiation throughout all Azure production environments. Access to production Azure clouds is requested via the CorpNet alias, ensuring identity proofing is implemented across all clouds. This alias is consistent across all a user's accounts in all Microsoft domains. All Azure access requests and approvals leverage these CorpNet aliases. New Azure user accounts refer to identities of existing Microsoft users using their unique CorpNet identifiers, known as aliases, who require access to Azure resources. The validation is conducted virtually by the third-party vendor, HireRight. Their responsibility is to perform background checks and verify government-issued IDs prior to the issuance of CorpNet aliases to Microsoft personnel. This process ensures the integrity and security of Microsoft Azure operations.  Azure smart cards tied to the specific environment of access are shipped via FedEx in a deactivated state and cannot be used until they are activated. A note is added to the user's account confirming the shipping number for tracking. Shipments require a signature for delivery. Smart cards are not activated until Core Services Engineering and Operations (CSEO) receives a confirmation email from the recipient, recipient's manager, AAM, or Security, ensuring the user's alias is consistent and validating the user's identity. The recipient must email the ticketing team from their Microsoft corporate email. The ticketing team provides the response. The smart card team works with the recipient to unlock their smart card via the ticketing tool. If the user is located in the Puget Sound region, they must come to the main Microsoft campus to pick up their smart card. If the user is outside of the Puget Sound region, the smart card is shipped directly to the individual and auto-disabled until activated by the user. |

# Incident Response (IR)

## IR-1 Policy and Procedures

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (OneOrMore): organization-level;mission/business process-level;system-level] incident response policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the incident response policy and the associated incident response controls;

b. Designate an [an official to manage the incident response policy and procedures is defined;] to manage the development, documentation, and dissemination of the incident response policy and procedures; and

c. Review and update the current incident response:

1. Policy [at least annually] and following [events that would require the current incident response policy to be reviewed and updated are defined;] ; and

2. Procedures [at least annually] and following [significant changes].

|  |
| --- |
| **IR-1 Control Summary Information** |
| Responsible Roles: Incident Response |
| Parameter ir-1(a): all personnel |
| Parameter ir-01\_odp.01: |
| Parameter ir-01\_odp.02: |
| Parameter ir-01\_odp.03: a Microsoft-wide |
| Parameter ir-01\_odp.04: the Microsoft Information Risk Management Council (IRMC) organization |
| Parameter ir-01\_odp.05: at least annually |
| Parameter ir-01\_odp.06: significant changes |
| Parameter ir-01\_odp.07: at least annually |
| Parameter ir-01\_odp.08: significant changes |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☒ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **IR-1 What is the solution and how is it implemented?** |
| **Part A1**  **Customer Responsibility**  The customer is responsible for developing, documenting, and disseminating incident response policy and procedures that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.  **Azure**  Azure addresses the incident management policy as part of the Microsoft security policies, of which there are two sets: the Microsoft Security Policy (MSP) that is applicable to all personnel, and the Microsoft Security Program Policy (MSPP), which is applicable to all personnel that have a responsibility for security. The Microsoft Information Risk Management Council (IRMC) is the governance body with review and approval responsibility for the MSP and MSPP. Within Azure, the MSPP specifically applies to all personnel involved in designing, building, and operating Azure and across all information and processes used in the conduct of Microsoft business. All Azure personnel are accountable and responsible for complying with these guiding principles within their designated roles. The policy addresses the following:  \* Incident management  \* Procedures and training  \* Incident evidence  \* Incident management capabilities  Additionally, the policy addresses the purpose, scope, roles, responsibilities, compliance requirements, and required coordination among the various Microsoft organizations that provide some level of support to all services. The policies indicate Microsoft management’s commitment and are a component of the risk management strategy which provides Azure personnel with a current set of clear and concise information security requirements.  The MSP is available to all Microsoft personnel on the Microsoft Policy website on the Microsoft intranet, and the MSPP and Security Standards are available through the Liquid tool, also on the Microsoft intranet. The Azure SOPs are stored in the Azure Security, Privacy & Compliance SharePoint site. This SharePoint site is accessible to all Azure personnel.  Service teams may supplement the Azure policies and procedures with offering-specific policies and procedures. Service-team-specific policies and procedures associated with incident management are documented and stored within internal Azure SharePoint sites. Only personnel with authorized credentials, adequate levels of permission, legitimate need to know, and specific roles and responsibilities are given access to the service-team-specific policies or procedures. |
| **Part A2**  **Customer Responsibility**  The customer is responsible for procedures to facilitate the implementation of the incident response policy and the associated incident response controls.  **Azure**  The Azure Incident Management Standard Operating Procedure (SOP) implements the incident management policy and associated controls and documents the following procedures:  \* Notification processes  \* Security incident data collection and analysis processes  \* A security incident documentation template and repository  \* An internal and external communication plan  \* Recovery procedures for system failures, data corruption, loss or denial of service, and total service compromise incidents  \* A process for post-mortem analysis  Service teams may supplement the Azure policies and procedures with offering-specific policies and procedures. Service-team-specific policies and procedures associated with incident management are documented and stored within internal Azure SharePoint sites. Only personnel with authorized credentials, adequate levels of permission, legitimate need to know, and specific roles and responsibilities are given access to the service-team-specific policies or procedures. |
| **Part B**  **Customer Responsibility**  The customer is responsible for designating an official to manage the development, documentation, and dissemination of the incident response policy and procedures.  **Azure**  The Microsoft Information Risk Management Council (IRMC) organization is the governance body with approval responsibility for the Microsoft Security Policy (MSP) and Microsoft Security Program Policy (MSPP). The IRMC consists of representatives from security and risk management teams across Microsoft including Core Services Engineering and Operations (CSEO), Azure, and Global Security. The Customer Security and Trust: Security Engineering (CST-SE) organization manages the review and approval process and maintains the policies.  On an annual basis, the CST-SE conducts a line-by-line review of the MSP and MSPP. The Microsoft Security Policy (MSP) and Microsoft Security Program Policy (MSPP) Governance document describes each member’s role, types and frequency of review, escalation paths, approval process, and formal publishing procedures of the security policy. Throughout the year, if necessary, CST-SE may convene with the IRMC to conduct reviews after a significant review or change request. The approved policy update is published within the relevant tool on the Microsoft intranet. If service teams establish service-specific or team-specific policies, the respective service teams update the necessary policies at least annually. |
| **Part C1**  **Customer Responsibility**  The customer is responsible for reviewing and updating the current incident response policy on a regular basis and following organization defined events.  **Azure**  The Azure team updates the Azure SOPs at least annually through a formal review process. If needed, the Azure team updates the SOP after a significant change affecting policy execution as well. If established, service-team-specific procedures are updated by their respective teams. The individual service teams review and update their respective SOPs at least annually and when required by a significant change. |
| **Part C2**  **Customer Responsibility**  The customer is responsible for reviewing and updating current incident response procedures on a regular basis and following organization defined events.  **Azure**  The Azure team updates the Azure SOPs at least annually through a formal review process. If needed, the Azure team updates the SOP after a significant change affecting policy execution as well. If established, service-team-specific procedures are updated by their respective teams. The individual service teams review and update their respective SOPs at least annually and when required by a significant change. |

## IR-2 Incident Response Training

a. Provide incident response training to system users consistent with assigned roles and responsibilities:

1. Within [ten (10) days for privileged users, thirty (30) days for Incident Response roles] of assuming an incident response role or responsibility or acquiring system access;

2. When required by system changes; and

3. [at least annually] thereafter; and

b. Review and update incident response training content [at least annually] and following [events that initiate a review of the incident response training content are defined;].

|  |
| --- |
| **IR-2 Control Summary Information** |
| Responsible Roles: Incident Response |
| Parameter ir-02\_odp.01: as part of onboarding |
| Parameter ir-02\_odp.02: at least annually or whenever a significant change occurs |
| Parameter ir-02\_odp.03: at least annually |
| Parameter ir-02\_odp.04: |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **IR-2 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for providing incident response training to users of customer-deployed resources in accordance with assigned roles and responsibilities and when changes occur.  **Azure**  Microsoft provides training annually to all Azure personnel on how to recognize, respond to, and report incidents as part of the basic security awareness training provided via the Security and Privacy Foundations and STRIKE training. As documented in the Azure Incident Management Standard Operating Procedure (SOP), incident managers ensure that all personnel, including new hires, are trained on incident handling procedures and protocols consistent with assigned roles and responsibilities.  This training is comprised of on-the-job oversight by current members of the Security Response Team. The Security Response Team uses job shadowing of real incidents and Azure Red Team engagements due to the centralized nature of the incident management function in Azure and the availability of job-shadowing within the Security Response Team. Live, ongoing, on-the-job training provides a more thorough and realistic incident management training environment by indoctrinating all stakeholders with the incident management procedures in real time. After a period of apprenticeship, generally around sixty days, the Security Response Team provides unaccompanied access to all necessary services, if appropriate. While there is no specific annual refresher course in incident management, the Security Response Team is continuously trained through daily incident management activities, team meetings, and engagement with external organizations.  The following roles in Azure Incident Management require specific on-boarding training: Incident Engineer, Incident Manager, Security Incident Engineer, Security Incident Manager, and Communications Manager. Part of the training replicates a real incident and walks personnel through the incident management process. Additionally, incident management tests and exercises are considered in-place training and are used to support other onsite training for new employees and other support staff with incident roles. Personnel are not made aware that they are being tested during incident management tests.  As part of the service team-specific incident management procedures, each team provides additional information and training to provide an understanding of the team’s distinct responsibilities and accountabilities in support of incident management. Service teams designate incident management personnel or distribution lists as part of Service Tree configurations.  All Microsoft personnel receive refresher training on security on an annual basis as part of their regular security awareness training. Service team on-call personnel receive additional training on their incident management roles and responsibilities through exercises and actual incident handling. Security Response Team members respond to incidents daily and commonly hold various industry certifications which require annual Continuing Professional Education (CPE) credits.  Employees with security-relevant roles receive refresher training on security on an annual basis, as part of their regular security training. Service team and feature team on-call personnel receive additional, in-place, training on their incident management roles and responsibilities through mandatory exercises conducted annually. |
| **Part B**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for reviewing and updating incident response training content to users of customer-deployed resources, when changes occur, in accordance with customer defined time periods.  **Azure**  As changes to Azure assets and procedures occur, Azure management considers whether additional incident management training is needed. If so, the training is developed and provided to applicable personnel. This includes training provided through on-the-job requirements, Azure Incident Management Standard Operating Procedure (SOP) updates, and team meetings. |

### IR-2(1) - Simulated Events

Incorporate simulated events into incident response training to facilitate the required response by personnel in crisis situations.

|  |
| --- |
| **IR-2(1) Control Summary Information** |
| Responsible Roles: Incident Response |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☒ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **IR-2(1) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for providing incident response training, which incorporates simulated events, to users of customer-deployed resources in accordance with assigned roles and responsibilities.  **Azure**  Service teams include Azure Red Team exercises as part of incident management training. Azure Red Team exercises using approved penetration testing tools are intended to identify weaknesses in the existing incident management processes. Incident tests and exercises are considered in-place training and are used to support other onsite training for new personnel with incident roles.  Service teams include tabletop and functional exercises as part of incident management training. Part of the training replicates a real incident and walks personnel through the incident management process. Additionally, incident management tests and exercises are considered in-place training and are used to support other onsite training for new employees and other support staff with incident roles. Personnel are not made aware that they are being tested during incident management tests.  As part of the service team-specific incident management procedures, each team provides additional information and training to provide an understanding of the team’s distinct responsibilities and accountabilities in support of incident management.  The Security Response Team uses job shadowing of real and Azure Red Team incidents due to the centralized nature of the incident management function in Azure and the availability of job-shadowing within the Security Response Team. Live, ongoing, on the job training provides a more thorough and realistic security incident management training environment by indoctrinating all stakeholders with the incident management procedures in real time. Azure considers job shadowing of live incidents a preferred and more effective alternative to simulated training mechanisms.  As part of the service team-specific incident management procedures, each team provides additional information and training to provide an understanding of the team’s distinct responsibilities and accountabilities in support of incident management. |

### IR-2(2) - Automated Training Environments

Provide an incident response training environment using [automated mechanisms used in an incident response training environment are defined;].

|  |
| --- |
| **IR-2(2) Control Summary Information** |
| Responsible Roles: Incident Response |
| Parameter ir-02.02\_odp: Organization-defined automated mechanisms |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☒ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **IR-2(2) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for providing incident response training using automated mechanisms, to users of customer-deployed resources in accordance with assigned roles and responsibilities.  **Azure**  To provide a thorough and realistic environment, security incident management training occurs through on-the-job shadowing during real and Azure Red Team incidents affecting the production environment, with senior security incident responders training newer personnel to provide real world experience and situations for training purposes. Live, ongoing, on the job training provides a more thorough and realistic security incident management training environment by indoctrinating all stakeholders with the incident management procedures in real time. Azure considers job shadowing of live incidents a preferred and more effective alternative to automated training mechanisms. |

## IR-3 Incident Response Testing

Test the effectiveness of the incident response capability for the system [at least every six (6) months, including functional at least annually] using the following tests: [tests used to test the effectiveness of the incident response capability for the system are defined;].

Requirement: The service provider defines tests and/or exercises in accordance with NIST Special Publication 800-61 (as amended). Functional testing must occur prior to testing for initial authorization. Annual functional testing may be concurrent with required penetration tests (see CA-8). The service provider provides test plans to the JAB/AO annually. Test plans are approved and accepted by the JAB/AO prior to test commencing.

|  |
| --- |
| **IR-3 Control Summary Information** |
| Responsible Roles: Incident Response |
| Parameter ir-03\_odp.01: at least every six (6) months |
| Parameter ir-03\_odp.02: tests and/or exercises in accordance with NIST Special Publication 800-61 Revision 2 |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **IR-3 What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for testing the incident response capability of customer-deployed resources.  **Azure**  Azure tests the incident management capability by using a process that is consistent with the NIST Special Publication 800-61 Revision 2. The Azure incident management capability is exercised by the Security Response Team on a regular basis as security incidents are identified and reported. In addition, Red Team exercises are utilized continuously to test and identify weaknesses in the incident management process using approved penetration testing tools. Lastly, regular mandatory exercises in coordination with contingency planning activities are performed at least annually.  All issues and action items identified during the exercise are documented in an incident tracking system and worked on until resolved. During the post-exercise phase, lessons learned are discussed and incident management policies and procedures are updated accordingly.  After the exercises, a post-exercise summary is documented. The post-exercise summary documents the incident ticket number which details how Azure determined there was an incident all the way through the resolution of the incident. Each incident entry is documented in an incident tracking system including identifying the personnel that made updates to the ticket.  The Security Response Team regularly evaluates response methodology and tools to ensure optimal performance during incidents in Azure as part of the Post incident management (PIR) process. |

### IR-3(2) - Coordination with Related Plans

Coordinate incident response testing with organizational elements responsible for related plans.

|  |
| --- |
| **IR-3(2) Control Summary Information** |
| Responsible Roles: Incident Response |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **IR-3(2) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for coordinating incident response testing with related plans (e.g., business continuity, contingency, disaster recovery).  **Azure**  The Azure Security Response Team coordinates incident handling activities with contingency planning activities managed by the Business Continuity Management (BCM) team. If incidents or incident management tests trigger Azure Business Continuity Plan (BCP) and/or Azure Disaster Recovery Plan (DRP) activation criteria, contingency plans are followed in coordination with the Azure Incident Management Standard Operating Procedure (SOP).  Incident response testing activities are also coordinated with service teams through table top and Azure Red Team exercises. These exercises are intended to replicate a real incident using approved penetration testing tools and identify weaknesses in the existing incident response processes. If incidents or incident response tests trigger contingency plan activation criteria, contingency plans are followed in coordination with the Azure Incident Management Standard Operating Procedure (SOP). |

## IR-4 Incident Handling

a. Implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery;

b. Coordinate incident handling activities with contingency planning activities;

c. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly; and

d. Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization.

Requirement: The FISMA definition of \"incident\" shall be used: \"An occurrence that actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.\"

Requirement: The service provider ensures that individuals conducting incident handling meet personnel security requirements commensurate with the criticality/sensitivity of the information being processed, stored, and transmitted by the information system.

|  |
| --- |
| **IR-4 Control Summary Information** |
| Responsible Roles: Incident Response |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **IR-4 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for implementing key incident handling capabilities including preparation, detection and analysis, containment, eradication, and recovery. In addition, incident handling for customer applications is the responsibility of the government agency unless caused by Microsoft or an incident is the result of Microsoft action. The government agency is responsible for providing a point of contact and escalation plan so that Microsoft keeps government staff informed during an incident response.  **Azure**  Azure implements a standardized incident handling framework derived from multiple incident handling methodologies including NIST Special Publication 800-61 Revision 2, ISO/IEC 27035:2011, and the SANS Institute publication Computer Security Incident Handling.  The Azure C+AI Incident Management process includes multiple stages throughout the resolution of an incident. Incidents may be managed with the Crisis Management or Security Customer Reportable Security or Privacy Incident sub-processes of the overarching Incident Management process. When incidents become triaged as a high severity event (Severity 1 or higher, Severity 0 being the highest) they are managed with the Customer Reportable Security or Privacy Incident sub-process. The process includes steps for preparation, detection and analysis, containment, eradication, and recovery and post-incident activity. Full investigations are conducted by the Security Response Team investigators and are overseen by a Security Incident Manager; this is accomplished through the forensic retrieval of data from affected assets and/or retrieval of relevant event data. Azure ensures individuals that are part of the Security Response Team meet personnel security requirements commensurate with the criticality and sensitivity of the information being processed, stored, and transmitted in Azure.  Azure actively plans and implements sustainable security incident management capabilities. incident management activities are reviewed regularly and improvements for infrastructure protection are identified to improve incident management capabilities.  Azure ensures individuals that are part of the Security Response Team meet personnel security requirements commensurate with the criticality and sensitivity of the information being processed, stored, and transmitted in Azure.  Additionally, Azure reports confirmed security and availability incidents to DoD, US-CERT and affected customers in accordance with applicable policies and procedures. |
| **Part B**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for coordinating incident handling activities with contingency planning activities for customer-deployed resources.  **Azure**  During the incident management assessment stage and throughout the incident handling process, the Security Response Team evaluates the incident’s severity and works with the affected service teams to initiate the appropriate Azure Business Continuity Plan (BCP) or Azure Disaster Recovery Plan (DRP).  As part of the Enterprise Business Continuity Management (EBCM) process followed by the service teams, the contacts for required incident management processes are included for business continuity and disaster recovery (BCDR). For planned BCDR activities, service teams use Incident Management (IcM) to track the activity. If related to an unplanned incident, the service teams use IcM to track the incident to closure. |
| **Part C**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for implementing incident handling capabilities that include lessons learned from ongoing incident handling activities; their incorporation into incident response procedures, training, and testing and the implementation of the resulting changes.  **Azure**  As part of IcM, when an incident is resolved, service teams must provide a resolution. When the incident is addressed, the service team with the incident ticket assigned to them resolves the incident and provides the mitigation steps taken to resolve the incident. Service teams can also provide root cause information for optionally correlating the incidents within IcM.  For all Severity 0, 1, or 2 incidents, a Post Incident Response (PIR) review is completed by the Security Response Team to determine root cause details and compile a report containing all lessons learned from the incident. The goals of these reviews are to:  \* Identify technical or communications lapses, procedural failures, manual errors, process flaws that might have caused the Availability Incident or that were identified with a formal PIR  \* Ensure technical lapses are captured and can be followed up with engineering teams in the form of bugs in their operational databases  \* Evaluate response procedures for sufficiency and completeness of operating procedures.  Additionally, the Incident Manager is accountable for maintaining an inventory of all repair items, their owners, and completion dates. The PIR should contain the following:  \* Customer/Business Impact  \* Incident Severity  \* Root Cause Description  \* Repair items  The concepts derived from the lessons learned, as mentioned above, are consistently incorporated into Microsoft Azure Incident Response training and testing procedures. This is achieved through continuous on-the-job shadow training and annual Strike, Security & Privacy Foundations Training. The ongoing on-the-job shadow training, which involves learning from real incidents, coupled with our annual Strike, Security & Privacy Foundations Training, is meticulously designed to fulfill the intent of the control. |
| **Part D**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for ensuring the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization.  **Azure**  The Security Response Team tracks all incidents affecting Azure; collects data about each incident as well as Post Incident Reports; and analyzes the gathered data to enhance the understanding of incident awareness and response across Azure.  The team performs monthly metric reviews and weekly post-mortems which correlates incident information and individual incident managements. The monthly metrics provide a better understanding and perspective of the threats against applications, people, and assets.  The Azure Incident Management Standard Operating Procedure (SOP) describes the incident handling process for all incidents, including incidents generated by insider threats. Azure Security may engage the Microsoft personnel investigations team to provide support and guidance on forensic investigations when the scope of investigation includes personnel working at Microsoft. Once an incident is identified as suspected insider threat, the Security Incident Manager notifies the Office of Legal Compliance (OLC). |

### IR-4(1) - Automated Incident Handling Processes

Support the incident handling process using [automated mechanisms used to support the incident handling process are defined;].

|  |
| --- |
| **IR-4(1) Control Summary Information** |
| Responsible Roles: Incident Response |
| Parameter ir-04.01\_odp: organization-defined automated mechanisms |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **IR-4(1) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for supporting incident handling processes using automated mechanisms (e.g., ticketing systems and incident tracking/reporting systems).  **Azure**  Azure employs automated mechanisms, including, but not limited to, service team-specific SharePoint and Microsoft Teams sites, Incident Management (IcM), and Service Now (SNow), the security ticket management system, to support the incident handling process such as alerts, notifications, error messages, or other automated warnings through the audit and accountability processes.  Upon identification of an incident, service teams create IcM tickets for tracking purposes. The team primarily responsible for resolution takes ownership of the IcM ticket and may create a ticket in Azure DevOps for secondary tracking. These are technical solutions that are available to personnel twenty-four (24) hours a day, seven (7) days a week. Due to the sensitive nature of security incidents, a separate ticketing system, SNow, is employed by the Security Response Team to track and manage security cases. SNow is used in addition to IcM and other tools to provide least privilege and need-to-know implementations.  If the incident is security related, the service team may transfer ownership of the IcM ticket, use the “Request Assistance” feature, or report via email to the Security Response Team twenty-four (24) hours a day, seven (7) days a week. |

### IR-4(2) - Dynamic Reconfiguration

Include the following types of dynamic reconfiguration for [all network, data storage, and computing devices] as part of the incident response capability: [types of dynamic reconfiguration for system components are defined;].

|  |
| --- |
| **IR-4(2) Control Summary Information** |
| Responsible Roles: BCDR |
| Parameter ir-04.02\_odp.01: types of dynamic reconfiguration |
| Parameter ir-04.02\_odp.02: all network, data storage, and computing devices |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **IR-4(2) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for including dynamic reconfiguration of all customer-deployed resources as part of the incident response capability (e.g., filter rules to firewalls and gateways, access control lists).  **Azure**  Azure personnel are able to access network, data storage, and computing devices within the system and change their configuration as required during the incident management process, up to and including updating firewall rules, restricting network access, removing users, and more. The Security Response Team maintains the capability to dynamically reconfigure information system components as outlined in the Rapid Containment Protocol section of the C+AI Security Playbooks. Capabilities include the ability to disable accounts, change ACLs and quarantine assets if determined necessary in an incident management scenario. |

### IR-4(4) - Information Correlation

Correlate incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.

|  |
| --- |
| **IR-4(4) Control Summary Information** |
| Responsible Roles: Incident Response |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **IR-4(4) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for correlating incident information and individual incident responses across the customer organization in order to achieve perspective on incident awareness and response.  **Azure**  The Security Response Team tracks all incidents affecting Azure; collects data about each incident as well as Post Incident Reports; and analyzes the gathered data to enhance the understanding of incident awareness and response across Azure.  The team performs monthly metric reviews and weekly post-mortems which correlates incident information and individual incident managements. The monthly metrics provide a better understanding and perspective of the threats against applications, people, and assets. |

### IR-4(6) - Insider Threats

Implement an incident handling capability for incidents involving insider threats.

|  |
| --- |
| **IR-4(6) Control Summary Information** |
| Responsible Roles: Incident Response |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **IR-4(6) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for implementing an incident handling capability for insider threats.  **Azure**  The Azure Incident Management Standard Operating Procedure (SOP) describes the incident handling process for all incidents, including incidents generated by insider threats. Azure Security may engage the Microsoft personnel investigations team to provide support and guidance on forensic investigations when the scope of investigation includes personnel working at Microsoft. Once an incident is identified as suspected insider threat, the Security Incident Manager notifies the Office of Legal Compliance (OLC).  Additionally, Azure Security may engage the Microsoft Corporate Security team to provide support and guidance on forensic investigations when the scope of investigation includes personnel working at Microsoft to include CorpNet information. |

### IR-4(11) - Integrated Incident Response Team

Establish and maintain an integrated incident response team that can be deployed to any location identified by the organization in [the time period within which an integrated incident response team can be deployed is defined;].

|  |
| --- |
| **IR-4(11) Control Summary Information** |
| Responsible Roles: Incident Response |
| Parameter ir-04.11\_odp: near real-time |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **IR-4(11) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for establishing and maintaining an integrated incident response team that can be deployed to any location identified by the organization in near real-time.  **Azure**  The Azure Security Response Team consisting of Microsoft Issues & Crisis Management, Security CELA, C+AI Compliance Team, National Security Team, Security Response Team, includes access to forensic/malicious code analysts, tool developers, and operators either directly or within Microsoft to share information and leverage knowledge of various functions to rapidly response to incidents in near real time. Azure locations generally include members of the Security Response Team, but given the interconnected nature of the hyperscale Azure cloud, physical access is rarely required for incident response. |

## IR-5 Incident Monitoring

Track and document incidents.

|  |
| --- |
| **IR-5 Control Summary Information** |
| Responsible Roles: Incident Response |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **IR-5 What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for tracking ans documenting incidents of customer-deployed resources.  **Azure**  The Azure Security Response Team utilizes the Incident Management (IcM) ticketing system for notification about new alerts. Certain Azure monitoring tools such as Azure Security Monitoring (ASM) create tickets automatically when monitoring for security events. These tickets can be assigned to the Security Response Team as necessary. In other cases, tickets are created as a result of manual log review, incident reporting from service teams, or incident management team research and investigation. Should an IcM alert pass the triage phase without being determined to be a false positive, the Security Response Team creates a case in Service Now (SNow), the security incident tracking tool. Case tickets are updated as more information on the incident is gathered.  While not preferred, the Azure Security Response Team monitors a dedicated phone and email alias twenty-four (24) hours a day, seven (7) days a week which can also be used to report suspected security issues. Tickets for events are entered into IcM and SNow and escalated as necessary. This escalation process enables incidents to be escalated to the proper teams. At any point in the escalation path, once the incident has been resolved, the responding support group updates the status of the incident. If it is a customer-related incident, the owner of the incident communicates the resolution of the issue to the customer. |

### IR-5(1) - Automated Tracking, Data Collection, and Analysis

Track incidents and collect and analyze incident information using [Assignment: organization-defined automated mechanisms].

|  |
| --- |
| **IR-5(1) Control Summary Information** |
| Responsible Roles: Incident Response |
| Parameter ir-5.1\_prm\_1: organization-defined automated mechanisms |
| Parameter ir-05.01\_odp.01: |
| Parameter ir-05.01\_odp.02: |
| Parameter ir-05.01\_odp.03: |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **IR-5(1) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for employing automated mechanisms to track security incidents and collecting and analyze incident information.  **Azure**  Incident Management (IcM) collects alerts which are then sent to incident management personnel as needed, who then generate a ticket in Service Now (SNow) to track the incident to resolution. |

## IR-6 Incident Reporting

a. Require personnel to report suspected incidents to the organizational incident response capability within [US-CERT incident reporting timelines as specified in NIST Special Publication 800-61 (as amended)] ; and

b. Report incident information to [authorities to whom incident information is to be reported are defined;].

Requirement: Reports security incident information according to FedRAMP Incident Communications Procedure.

|  |
| --- |
| **IR-6 Control Summary Information** |
| Responsible Roles: Incident Response |
| Parameter ir-06\_odp.01: incident categorization and reporting timelines as specified in NIST Special Publication 800-61 |
| Parameter ir-06\_odp.02: the appropriate CIRT/CERT, the customer, and/or law enforcement as documented in the Azure Incident Management Standard Operating Procedure (SOP) |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **IR-6 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  The customer is responsible for requiring personnel to report suspected security incidents to the organizational incident management capability within the required time period.  **Azure**  All Microsoft personnel are required to immediately report events when they believe that a security incident has occurred. Examples of such events include, but are not limited to:  \* Alerts, notifications, error messages, or other automated warnings that indicate a security incident may have occurred.  \* Reports of security incidents received from external parties, including customers, members of the press, or the general public.  \* Personal observations of anomalies or unexpected events that might indicate a security incident has occurred.  \* Indication of virus, malicious software or hacker activity.  Personnel can report incidents by manually entering event related data directly into the incident management ticketing system which is classified in accordance with NIST Special Publication 800-61 Revision 2 standards based on the Classification, Escalation, and Notification (CEN) Matrix and escalated or by sending email to cdoc@microsoft.com. Tickets are routed automatically to the Security Response Team.  Any incident that involves the breach of personal information (PII or above) also requires a notification to the Security team at alias cdoc@microsoft.com. Security then loops in the dedicated Privacy team if needed. Incidents that involve the exposure of information covered by the Microsoft Privacy Policy necessitate the involvement of the Privacy team. |
| **Part B**  **Customer Responsibility**  The customer is responsible for reporting security incident information.  Per contractual agreement, it is the customer’s responsibility to provide accurate and current contact information to Azure to receive notifications of security incidents involving the potential breach of customer data. The customer is also responsible to designate the necessary parties as notification contacts.  It is the responsibility of the government customer agencies to inform Microsoft of the individuals, teams, and email addresses to be notified and kept updated for the incident handling process. Upon a confirmed security incident, Azure Security Response notifies the Administrators and Co-Administrators of a subscription. It is the responsibility of the customers to notify the appropriate parties if a breach occurs entirely within the customer’s scope of responsibility (e.g. if a customer VM is breached due to a poor password).  **Azure**  The Azure Security team coordinates with the ISSO to notify the appropriate contacts including, as appropriate, authorizing officials, customers, and others, of an incident, incident updates, and resolution. Azure reports events per the timelines and process are documented in the Azure Incident Management Standard Operating Procedure (SOP) . The Azure Incident Management Standard Operating Procedure (SOP) identifies the types of security incidents that should be reported to the regulator or regulators, reporting timeframes, and specific processes for reporting and handling incidents involving customer data.  Customers receive notification of security incidents involving the confirmed breach of their customer data via means Microsoft deems most appropriate. This is via email sent to the administrators and co-administrators of an impacted subscription or through updates to the Service Health Dashboard, or the customer’s Azure Management Portal within the times periods defined in the Azure Incident Management Standard Operating Procedure (SOP). |

### IR-6(1) - Automated Reporting

Report incidents using [automated mechanisms used for reporting incidents are defined;].

|  |
| --- |
| **IR-6(1) Control Summary Information** |
| Responsible Roles: Incident Response |
| Parameter ir-06.01\_odp: organization-defined automated mechanisms |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **IR-6(1) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for employing automated mechanisms to support incident reporting (e.g., ticketing and incident tracking/reporting systems).  **Azure**  Azure automates incident reporting through use of Incident Management (IcM) connectors which trigger the creation of an incident via detection logic.  Azure Security Monitoring (ASM) and SCUBA are the primary automated monitoring services for security event reporting used within Azure. Any alerts or detections fired by ASM or SCUBA notify either the service team which owns the asset or the Security Response Team, depending on what is most appropriate, via IcM. |

### IR-6(3) - Supply Chain Coordination

Provide incident information to the provider of the product or service and other organizations involved in the supply chain or supply chain governance for systems or system components related to the incident.

|  |
| --- |
| **IR-6(3) Control Summary Information** |
| Responsible Roles: Incident Response, Supply Chain |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **IR-6(3) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for providing incident information to providers of products or services and other supply chain organizations for incidents related to customer-deployed resources.  **Azure**  As part of Microsoft Supply Chain Security Program, Azure deploys a team responsible for leading and supporting supply chain risk management activities. The team members are introduced to industry-leading supply chain quality programs to support Azure cloud environments. The team members have established agreements and procedures with various Azure partner teams of supply chain such as Azure Security, Azure Federal Compliance, and CELA teams for the notification of supply chain compromises and findings that are a result of assessments. If findings are identified, stakeholders of Azure cloud environments are notified through the approval of CELA on communication plans. Remediation plans for supply chain compromises or findings during assessments are formulated to track until implementation by team members who lead and support supply chain risk management activities. |

## IR-7 Incident Response Assistance

Provide an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the system for the handling and reporting of incidents.

|  |
| --- |
| **IR-7 Control Summary Information** |
| Responsible Roles: Incident Response |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **IR-7 What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for providing incident response support resources that are integral to the organizational incident response capability, providing advice and assistance to users handling incidents.  **Azure**  For all asset types, Azure implements both internal and external sites which offer advice and assistance to Azure personnel and customers for handling and reporting of security incidents. Azure sites are supported on SharePoint and internal access is granted to appropriate personnel.  **Internal**  Azure policies and procedures are distributed and published to a central SharePoint repository and are accessible to all Azure personnel. The Azure Security Response Team provides regular updates around event triage and incident management which are available to all applicable Azure incident management personnel.  Azure use the services of the Microsoft Security Response Center (MSRC) working in the Cyber Defense Operations Center (CDOC) to manage incident questions and reporting by Microsoft personnel. Microsoft personnel can report incidents using the email alias <cdoc@microsoft.com> or via Incident Management (IcM) which is then routed to the appropriate Azure team.  Internal web pages offer advice and assistance to service teams for the handling and reporting of security incidents. These web pages provide the following information to Azure personnel:  \* What are security incidents  \* How to identify such incidents  \* How to escalate the security incidents  \* List of sample security incidents  \* Who to contact in the event of a security incident  The Azure Security Response Team also posts a phone number and email alias on their internal website. This contact information is provided for service team personnel to use when required to file a security incident. Additionally, security contact information is available as part of IcM.  Depending on the nature of the incident, Azure may engage subject matter experts (SMEs) from other organizations within Microsoft to facilitate investigative needs.  **External**  The Azure Trust Center describes how to submit a security incident in Azure. The Microsoft Docs webpage also provides support to customers and links them to a wide variety of web pages which provide guidance around information security incidents related to their cloud environment and customer support, if needed.  Customers can report security events at any time through the customer support website handled by Customer Support Services (CSS). CSS routes it to appropriate service team. In addition, possible security incidents and abuse can be reported on <https://cert.microsoft.com/>. These reports are received by the Online Services Security and Compliance Security team and then routed to the appropriate service team to investigate and correct the event. There is also a dedicated phone line that is available on a twenty-four (24) hours a day, seven (7) days a week basis to report events at 1-866-676-6546.  Working with the C+AI Security Response Team, external parties such as law enforcement, Information Security Programs (ISPs), and other partners can identify security issues. For example, the Global Infrastructure Alliance for Internet Security (GIAIS) utilizes the Microsoft Security Response Alliance to feed security concerns to Microsoft’s online services which is then routed to the appropriate Azure service teams. |

### IR-7(1) - Automation Support for Availability of Information and Support

Increase the availability of incident response information and support using [automated mechanisms used to increase the availability of incident response information and support are defined;].

|  |
| --- |
| **IR-7(1) Control Summary Information** |
| Responsible Roles: Incident Response |
| Parameter ir-07.01\_odp: organization-defined automated mechanisms |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **IR-7(1) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for using automated mechanisms to increase the availability of incident response support resources.  **Azure**  Azure tracks events and incidents through Incident Management system (IcM) and Service Now (SNow) and employs Azure Security Monitoring (ASM) and SCUBA within the environment in support of the incident management process. These services utilize automated mechanisms to identify incidents as well as document, track, and report incidents.  For high severity incidents, Azure Security maintains an internal notification wiki site on the central Microsoft Teams repository. Azure teams and individuals can sign up to receive automated email alerts when SharePoint content is added or modified. Internal web pages and troubleshooting guides offer advice and assistance to service team personnel for the handling and reporting of security incidents including the Azure Incident Management Standard Operating Procedure (SOP). |

## IR-8 Incident Response Plan

a. Develop an incident response plan that:

1. Provides the organization with a roadmap for implementing its incident response capability;

2. Describes the structure and organization of the incident response capability;

3. Provides a high-level approach for how the incident response capability fits into the overall organization;

4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;

5. Defines reportable incidents;

6. Provides metrics for measuring the incident response capability within the organization;

7. Defines the resources and management support needed to effectively maintain and mature an incident response capability;

8. Addresses the sharing of incident information;

9. Is reviewed and approved by [personnel or roles that review and approve the incident response plan is/are identified;] [at least annually] ; and

10. Explicitly designates responsibility for incident response to [entities, personnel, or roles with designated responsibility for incident response are defined;].

b. Distribute copies of the incident response plan to [see additional FedRAMP Requirements and Guidance];

c. Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing;

d. Communicate incident response plan changes to [see additional FedRAMP Requirements and Guidance] ; and

e. Protect the incident response plan from unauthorized disclosure and modification.

(b) Requirement: The service provider defines a list of incident response personnel (identified by name and/or by role) and organizational elements. The incident response list includes designated FedRAMP personnel.

(d) Requirement: The service provider defines a list of incident response personnel (identified by name and/or by role) and organizational elements. The incident response list includes designated FedRAMP personnel.

|  |
| --- |
| **IR-8 Control Summary Information** |
| Responsible Roles: Incident Response |
| Parameter ir-8(d): see additional FedRAMP Requirements and Guidance |
| Parameter ir-08\_odp.01: the Azure ISSO |
| Parameter ir-08\_odp.02: at least annually |
| Parameter ir-08\_odp.03: incident response personnel as documented within the Azure Incident Management Standard Operating Procedure (SOP), C+AI Security Operations Center (SOC), FedRAMP |
| Parameter ir-08\_odp.04: incident response personnel as documented within the Azure Incident Management Standard Operating Procedure (SOP), C+AI SOC, FedRAMP |
| Parameter ir-08\_odp.05: |
| Parameter ir-08\_odp.06: |
| Parameter ir-08\_odp.07: |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **IR-8 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  The customer is responsible for developing an incident response plan for customer-deployed resources.  **Azure**  Microsoft has developed and implemented the Azure Incident Management Standard Operating Procedure (SOP) which provides Azure a roadmap for implementing its incident management capability. The purpose is to provide guidance concerning the responsibilities of involved parties during any incident that affects the confidentiality, integrity, or availability of Azure. The document provides a high-level approach for how the incident management capability fits into the overall organization and describes the structure and organization of the incident management capabilities, including:  \* Describing the end-to-end process of security incident management, and how it is executed across the various functional groups within Microsoft.  \* Defining a methodical approach that may be applied to resolve security incidents and escalate incidents to the proper internal authorities.  The Azure Incident Management Standard Operating Procedure (SOP) explains the different phases of the incident management lifecycle. Details for each of the phases are explained in the plan. The document also identifies the internal partners, cross-team contacts, roles and responsibilities, and lists the individuals and management support needed to effectively maintain and mature the incident management capability.  The Azure Incident Management Standard Operating Procedure (SOP) provides guidance for classifying the incidents and assigning severity. It also provides the characteristics that could be associated with incidents to help categorize the incidents. Security incidents are tracked in a ticketing system where they are categorized and assigned a severity rating. Security incidents include, but are not limited to: e-mail viruses, rootkits, worms, denial of service attacks, unauthorized access, inappropriate use of network resources, any other type of unauthorized, unacceptable, unlawful activity involving Azure computer networks or data processing equipment, and compromise, disclosure, or use of information that occurs outside its intended purpose.  There are five phases in the Azure incident management lifecycle: detect, assess, diagnose, stabilize and recover, and close. The Azure Incident Management Standard Operating Procedure (SOP) meets the unique requirements of the organization, which relate to mission, size, structure, and functions.  The Microsoft Security Response Center (MSRC) is responsible for reporting on its efforts with Azure as a Quality of Service (QoS) Metric. Metrics are defined as the following:  \* Total Number of Incidents: The Security Response Team reports the total number of incidents experienced by online services and can report incidents with respect to incident category, property affected, and other dimensions.  \* Time to Detect (TTD): The time between when an incident began and when it was identified by the finder. This metric can only be determined after an investigation has been conducted by the Security Response Team.  \* Time to Engage (TTE): The time between when an incident is reported to Security Response Team and Security Response Team takes action.  \* Time to Mitigate (TTM): The time between when an incident is reported to Security Response Team and the incident is mitigated and/or resolved.  A formal Incident Report is produced by the service teams and augmented with the Azure Security Response Team’s additions. These reports, which include lessons learned, are created for all events with a Severity 1 rating. For incidents of lesser severity, if there are significant lessons learned that have general applicability across the Azure environment, an incident report is created. The incident reports are maintained by Azure Security incident management or by the impacted service team and are provided to the relevant stakeholders for review.  At a minimum, the Azure Incident Management Standard Operating Procedure (SOP) is reviewed and updated annually. Additionally, if applicable, post-incident response action items for incidents may trigger changes to be applied to the document and accompanying playbooks as required. |
| **Part B**  **Customer Responsibility**  The customer is responsible for distributing the incident response plan to incident response personnel.  **Azure**  The Azure Incident Management Standard Operating Procedure (SOP) is stored in a centralized SharePoint site. Azure uses SharePoint access controls to protect the document from unauthorized disclosure or modification. |
| **Part C**  **Customer Responsibility**  The customer is responsible for updating the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing.  **Azure**  Post-incident response action items for incidents may trigger changes to be applied to the Azure Incident Management Standard Operating Procedure (SOP) and accompanying playbooks as required. |
| **Part D**  **Customer Responsibility**  The customer is responsible for communicating changes made to the incident response plan.  **Azure**  After changes have been made to the Azure Incident Management Standard Operating Procedure (SOP), it is made available for review to Azure personnel via a centralized SharePoint site. |
| **Part E**  **Customer Responsibility**  The customer is responsible for protecting the incident response plan.  **Azure**  The Azure Incident Management Standard Operating Procedure (SOP) is stored in a centralized SharePoint site. Azure uses SharePoint access controls to protect the document from unauthorized disclosure or modification. |

## IR-9 Information Spillage Response

Respond to information spills by:

a. Assigning [personnel or roles assigned the responsibility for responding to information spills is/are defined;] with responsibility for responding to information spills;

b. Identifying the specific information involved in the system contamination;

c. Alerting [personnel or roles to be alerted of the information spill using a method of communication not associated with the spill is/are defined;] of the information spill using a method of communication not associated with the spill;

d. Isolating the contaminated system or system component;

e. Eradicating the information from the contaminated system or component;

f. Identifying other systems or system components that may have been subsequently contaminated; and

g. Performing the following additional actions: [actions to be performed are defined;].

|  |
| --- |
| **IR-9 Control Summary Information** |
| Responsible Roles: Incident Response, CELA |
| Parameter ir-09\_odp.01: incident response personnel as documented within the Azure Incident Management Standard Operating Procedure (SOP) |
| Parameter ir-09\_odp.02: incident response personnel as documented within the Azure Incident Management Standard Operating Procedure (SOP) |
| Parameter ir-09\_odp.03: actions documented within the Azure Incident Management Standard Operating Procedure (SOP) |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **IR-9 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  The customer is responsible for assigning individuals for responding to information spills.  **Azure**  The Azure Security Response Team consisting of Microsoft Cloud + AI Livesite, Privacy, and Security Teams, is responsible for responding to information spills. The team coordinates with service teams and partner groups in their response to an information spillage scenario. |
| **Part B**  **Customer Responsibility**  The customer is responsible for identifying customer-controlled information involved in the information contamination.  **Azure**  In the event of an information spill, Azure initiates the incident management process to identify the specific information involved in the spill, as well as the assets or networks affected. Procedures exist to ensure that Azure personnel impacted by information spills can continue to carry out assigned tasks while contaminated services are undergoing corrective actions. |
| **Part C**  **Customer Responsibility**  The customer is responsible for responding to information spills of customer-controlled data, including the personnel/roles to be alerted of the information spill and the usage of a communication method that is not associated with the spill.  **Azure**  The Azure incident management process includes notification of appropriate personnel as documented in the Azure Incident Management Standard Operating Procedure (SOP). |
| **Part D**  **Customer Responsibility**  The customer is responsible for responding to information spills, including how the contaminated customer-deployed resources are isolated.  **Azure**  In the instance of a contaminated asset or network, the Security Response Team isolates the spillage using rapid containment options available to properly address the reach of an information spillage. Some of the rapid containment options include powering off the asset, institute Border Gateway Protocol (BGP) black hole routing, and network configuration changes to contain the breach. |
| **Part E**  **Customer Responsibility**  The customer is responsible for responding to information spills, including the eradication of information from the contaminated customer-deployed resources.  **Azure**  Upon identification of Azure assets containing spilled information, Azure incident management personnel take steps to eradicate that information. After the information spillage is contained, a cleanup process is initiated. The cleanup process involves locating, isolating, and deleting the contaminated data. In addition, data zeroing would be completed, in order to ensure mirrored data to replica sites are also cleansed. |
| **Part F**  **Customer Responsibility**  The customer is responsible for responding to information spills of customer-controlled data, including the identification of other resources which may have been subsequently contaminated.  **Azure**  The process of identifying contaminated assets followed by Azure includes identification of other assets to which data may have been replicated, and if necessary, further investigation of those assets. |
| **Part G**  **Customer Responsibility**  The customer is responsible for defining and performing other customer-defined actions in response to information spills of customer-controlled data.  **Azure**  Azure incident management follows the incident management process in response to information spillage as documented in the Azure Incident Management Standard Operating Procedure (SOP). |

### IR-9(2) - Training

Provide information spillage response training [at least annually].

|  |
| --- |
| **IR-9(2) Control Summary Information** |
| Responsible Roles: Incident Response, CELA |
| Parameter ir-09.02\_odp: at least annually |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **IR-9(2) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for providing information spillage response training.  **Azure**  All personnel receive annual security training via Security and Privacy Foundations and STRIKE, which include information on incident management. Information spillage is treated as an incident within the incident management process. |

### IR-9(3) - Post-spill Operations

Implement the following procedures to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions: [procedures to be implemented to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions are defined;].

|  |
| --- |
| **IR-9(3) Control Summary Information** |
| Responsible Roles: Incident Response, CELA |
| Parameter ir-09.03\_odp: organization-defined procedures |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☒ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☒ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **IR-9(3) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for ensuring customer personnel impacted by information spills can continue carrying out assigned tasks.  **Azure**  The incident management information spill cleanup process does not require shutting down services or removing services from the network. Azure personnel are able to continue carrying out assigned tasks while contaminated services are undergoing corrective actions. |

### IR-9(4) - Exposure to Unauthorized Personnel

Employ the following controls for personnel exposed to information not within assigned access authorizations: [controls employed for personnel exposed to information not within assigned access authorizations are defined;].

|  |
| --- |
| **IR-9(4) Control Summary Information** |
| Responsible Roles: Incident Response, CELA |
| Parameter ir-09.04\_odp: security awareness training requiring incident reporting, signed NDAs |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **IR-9(4) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for employing controls for personnel exposed to information not within assigned access authorizations.  **Azure**  All Azure personnel have received security awareness training requiring the reporting of an incident if they are exposed to information not within their assigned access authorization and have signed an Employee Agreement that serve as a Non-Disclosure Agreements (NDA). |

# Maintenance (MA)

## MA-1 Policy and Procedures

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (OneOrMore): organization-level;mission/business process-level;system-level] maintenance policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the maintenance policy and the associated maintenance controls;

b. Designate an [an official to manage the maintenance policy and procedures is defined;] to manage the development, documentation, and dissemination of the maintenance policy and procedures; and

c. Review and update the current maintenance:

1. Policy [at least annually] and following [events that would require the current maintenance policy to be reviewed and updated are defined;] ; and

2. Procedures [at least annually] and following [significant changes].

|  |
| --- |
| **MA-1 Control Summary Information** |
| Responsible Roles: SOP Team, Policy |
| Parameter ma-1(a): all personnel |
| Parameter ma-01\_odp.01: |
| Parameter ma-01\_odp.02: |
| Parameter ma-01\_odp.03: a Microsoft-wide |
| Parameter ma-01\_odp.04: the Microsoft Information Risk Management Council (IRMC) organization |
| Parameter ma-01\_odp.05: at least annually |
| Parameter ma-01\_odp.06: significant changes |
| Parameter ma-01\_odp.07: at least annually |
| Parameter ma-01\_odp.08: significant changes |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☒ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **MA-1 What is the solution and how is it implemented?** |
| **Part A1**  **Customer Responsibility**  The customer is responsible for developing, documenting, and disseminating maintenance policy and procedures that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.  **Azure**  Azure addresses the system maintenance policy as part of the Microsoft security policies, of which there are two sets: the Microsoft Security Policy (MSP) that is applicable to all Microsoft personnel, and the Microsoft Security Program Policy (MSPP), which is applicable to all Microsoft personnel that have a responsibility for security. The Microsoft Information Risk Management Council (IRMC) is the governance body with review and approval responsibility for the MSP and MSPP. Within Azure, the MSPP specifically applies to all Microsoft personnel with security objectives such as designing, building, and operating Azure and across all information and processes used in the conduct of Microsoft business. All Azure personnel are accountable and responsible for complying with these guiding principles within their designated roles. The policy addresses the following:  \* Maintenance, utilities, and tools  \* Data integrity  Additionally, the policy addresses the purpose, scope, roles, responsibilities, compliance requirements, and required coordination among the various Microsoft organizations that provide some level of support to all services. The policies indicate Microsoft management’s commitment and are a component of the risk management strategy which provides Azure personnel with a current set of clear and concise information security requirements.  The MSP is available to all Microsoft personnel on the Microsoft Policy website on the Microsoft intranet, and the MSPP and Security Standards are available through the Liquid tool, also on the Microsoft intranet. The Azure SOPs are stored in the Azure Security, Privacy & Compliance SharePoint site. This SharePoint site is accessible to all Azure personnel.  Service teams may supplement the Azure policies and procedures with offering-specific policies and procedures. Service-team-specific policies and procedures associated with system maintenance are documented and stored within internal Azure SharePoint sites. Only personnel with authorized credentials, adequate levels of permission, legitimate need to know, and specific roles and responsibilities are given access to the service-team-specific policies or procedures. |
| **Part A2**  **Customer Responsibility**  The customer is responsible for procedures to facilitate the implementation of the maintenance policy and the associated maintenance controls.  **Azure**  The Physical and Environmental Security Standard​ implements the system maintenance policy and associated controls and documents the following procedures:  \* Maintenance activities  \* Authorized personnel  \* Maintenance tickets  Service teams may supplement the Azure policies and procedures with offering-specific policies and procedures. Service-team-specific policies and procedures associated with system maintenance are documented and stored within internal Azure SharePoint sites. Only personnel with authorized credentials, adequate levels of permission, legitimate need to know, and specific roles and responsibilities are given access to the service-team-specific policies or procedures. |
| **Part B**  **Customer Responsibility**  The customer is responsible for designating an official to manage the development, documentation, and dissemination of the maintenance policy and procedures.  **Azure**  The Microsoft Information Risk Management Council (IRMC) organization is the governance body with approval responsibility for the Microsoft Security Policy (MSP) and Microsoft Security Program Policy (MSPP). The IRMC consists of representatives from security and risk management teams across Microsoft including Core Services Engineering and Operations (CSEO), Azure, and Global Security. The Customer Security and Trust: Security Engineering (CST-SE) organization manages the review and approval process and maintains the policies.  On an annual basis, the CST-SE conducts a line-by-line review of the MSP and MSPP. The Microsoft Security Policy (MSP) and Microsoft Security Program Policy (MSPP) Governance document describes each member’s role, types and frequency of review, escalation paths, approval process, and formal publishing procedures of the security policy. Throughout the year, if necessary, CST-SE may convene with the IRMC to conduct reviews after a significant review or change request. The approved policy update is published within the relevant tool on the Microsoft intranet. If service teams establish service-specific or team-specific policies, the respective service teams update the necessary policies at least annually. |
| **Part C1**  **Customer Responsibility**  The customer is responsible for reviewing and updating the current maintenance policy on a regular basis and following organization defined events.  **Azure**  The Azure team updates the Azure SOPs at least annually through a formal review process. If needed, the Azure team updates the SOP after a significant change affecting policy execution as well. If established, service-team-specific procedures are updated by their respective teams. The individual service teams review and update their respective SOPs at least annually and when required by a significant change. |
| **Part C2**  **Customer Responsibility**  The customer is responsible for reviewing and updating the maintenance procedures on a regular basis and following organization defined events.  **Azure**  The Azure team updates the Azure SOPs at least annually through a formal review process. If needed, the Azure team updates the SOP after a significant change affecting policy execution as well. If established, service-team-specific procedures are updated by their respective teams. The individual service teams review and update their respective SOPs at least annually and when required by a significant change. |

## MA-2 Controlled Maintenance

a. Schedule, document, and review records of maintenance, repair, and replacement on system components in accordance with manufacturer or vendor specifications and/or organizational requirements;

b. Approve and monitor all maintenance activities, whether performed on site or remotely and whether the system or system components are serviced on site or removed to another location;

c. Require that [personnel or roles required to explicitly approve the removal of the system or system components from organizational facilities for off-site maintenance or repairs is/are defined;] explicitly approve the removal of the system or system components from organizational facilities for off-site maintenance, repair, or replacement;

d. Sanitize equipment to remove the following information from associated media prior to removal from organizational facilities for off-site maintenance, repair, or replacement: [information to be removed from associated media prior to removal from organizational facilities for off-site maintenance, repair, or replacement is defined;];

e. Check all potentially impacted controls to verify that the controls are still functioning properly following maintenance, repair, or replacement actions; and

f. Include the following information in organizational maintenance records: [information to be included in organizational maintenance records is defined;].

|  |
| --- |
| **MA-2 Control Summary Information** |
| Responsible Roles: Datacenter Hosting |
| Parameter ma-02\_odp.01: Datacenter Management, Property asset owners |
| Parameter ma-02\_odp.02: (i) the date and time of maintenance; (ii) name of the individual performing the maintenance; (iii) name of escort, if necessary; (iv) a description of the maintenance performed; and (v) a list of equipment removed or replaced (including identification numbers, if applicable) |
| Parameter ma-02\_odp.03: Maintenance records are retained in tracking tool |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **MA-2 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for scheduling, performing, documenting, and reviewing remote maintenance and repair records for all customer-deployed operating systems in accordance with organizational requirements.  **Azure**  Microsoft has two types of assets that must be maintained: Critical Environment (CE) and Site Services:  \* Critical Environments is the team that provides operation and maintenance of electrical, mechanical, and physical systems that comprise the operating infrastructure of the facility. Examples include generators, UPS, Fire Detection and Suppression systems, and HVAC systems.  \* Site Services is the team that provides the servicing of Microsoft online services assets (i.e., physical servers, network devices, etc.) located at the datacenter. The Site Services team provides break/fix and deployment services based on the issuance of a work ticket.  Microsoft captures maintenance records in the maintenance tracking tool for CE equipment and the workflow ticket tracking system for Site Services. The tool records the date and time of the maintenance, the name of the individual performing the maintenance along with details on the maintenance being performed, and any equipment being removed or replaced. If a particular maintenance activity required that someone be under escort in a restricted area, the name of the escort would be captured in the ticket.  **Critical Environment Equipment**  The Critical Environment (CE) team schedules, performs, documents, and reviews all maintenance activities performed on CE assets. Azure datacenters rely on a computerized maintenance management system to manage maintenance schedules and work order management. Microsoft Global Maintenance Standards which are a combination of OEM guidelines, NFPA708, IEEE, historical site data and expertise. Work orders are generated based on original equipment manufacturer (OEM) guidelines and assigned for completion. All maintenance work performed at an Azure datacenter must follow approved instructions captured in a Method of Procedure (MOP) document. A MOP must have datacenter management approval before work can begin. Completed MOPs are reviewed and receive datacenter management sign-off to indicate completion. Details of completed MOPs are stored in the appropriate workflow ticketing tool and then the work order is closed. The workflow ticketing tool is used to document and track all maintenance on CE equipment.  CE maintenance activities also require peer reviews of the MOPs as a verification of completeness and quality assurance. The peer reviews verify that any required configurations or security settings are correctly in place before completion of the maintenance. During monthly review meetings with the CE team, Datacenter Management reviews and verifies all CE work that was completed in the previous month.  **Site Services**  The Site Services team provides a smart hands and break fix service for assets belonging to properties provisioning services from the datacenter. For example, assets requiring physical maintenance could request smart hands service from the Site Services team. All Site Services work on assets is scheduled, performed, documented, and reviewed in work tickets within the workflow ticketing tool. No work can occur without an approved work ticket. The Site Services team follows detailed procedure documents that define step by step instructions for specific service requests. As part of the procedure documents, one of the final steps is to perform a Quality Control check to ensure that all steps were completed and that required security settings are in place. |
| **Part B**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for approving and monitoring of all remote maintenance activities performed on customer-deployed operating systems.  **Azure**  **Critical Environment Equipment**  Datacenter Management consists of Microsoft personnel who serve in the following roles: Datacenter Campus Director, Datacenter Operations Manager (DCOM), IT Operations Manager (ITOM), Critical Environment Operations Manager (CEOM), Senior Electrical Engineer (EE), Senior Mechanical Engineer (ME), Critical Environment Program Manager (CEPM), Instrumentation Engineer (IE), EHS Manager, Energy Marshall, and Datacenter Project Manager (DCPM). The CEOM, CEPM, EE and ME are responsible for work occurring in the DC critical environment. CE maintenance is prescribed in required step by step documents called Methods of Procedure (MOP). MOPs are reviewed and approved by datacenter management prior to any work beginning. MOPs serve as the checklist for the maintenance procedure and the documentation of the work completed. CE maintenance is performed in areas of the datacenter that are controlled and protected by physical security mechanisms, including, but not limited to, approved access, cameras, multifactor authentication, access smart cards, biometrics, and security patrols.  **Site Services**  The DCOM, ITOM and/or SOM are responsible for all Site Services work that occurs in the datacenter or for work that requires the asset to be transferred offsite. Site Services maintenance is performed in areas of the datacenter that are controlled and protected by physical security mechanisms (e.g. approved access, cameras, 2FA: access smart cards, biometrics, security patrols). |
| **Part C**  **Azure**  **Critical Environment Equipment**  If CE components are required to be removed from the facility, handling of the equipment is approved by Datacenter Management. In most instances, CE components receive onsite maintenance and are not removed from the facility.  **Site Services**  Property assets (e.g. Azure network device or server) requiring transfer offsite must have explicit asset owner (e.g. O365 asset owner) approval. |
| **Part D**  **Azure**  **Data Bearing Equipment and Site Services**  Assets that are to be destroyed are stored in locked storage bins that are under CCTV camera coverage. When the assets are ready to be destroyed, a physical security officer and a Microsoft full time employee (FTE) from Asset Management must escort the locked bin from the Azure colocation to where the onsite shredding is to occur. As shredding occurs at the datacenter and under Microsoft supervision, Azure assets do not leave the controlled areas of the datacenter. Any production device that is to be removed off-site with drives intact require a policy exception . |
| **Part E**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for identifying potentially impacted security controls and the process used for verifying those controls are still functioning properly following remote maintenance/repair activities on customer-deployed operating systems.  **Azure**  **Critical Environment Equipment**  CE maintenance activities also require peer reviews of the MOP checklist as a verification of completeness and quality assurance. The peer reviews verify that any required configurations or security settings are correctly in place before completion of the maintenance. During monthly review meetings with the CE team, Datacenter Management reviews/verifies all CE work that was completed in the previous month.  **Site Services**  The Site Services team follows detailed procedure documents that define step by step instructions for specific service requests. As part of the procedure documents, one of the final steps is to perform a Quality Control check to ensure that all steps were completed and that required security settings are in place. Any logical access required to Azure assets is performed per the authentication process. |
| **Part F**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for including customer-defined remote maintenance-related information for customer-deployed operating systems in organizational maintenance records.  **Azure**  Azure captures maintenance records in the workflow ticket tracking system for Site Services and the maintenance tracking tool for CE equipment. The tool records the date and time of the maintenance, the name of the individual performing the maintenance along with details on the maintenance being performed, and any equipment being removed or replaced. If a maintenance activity requires that someone be under escort in a restricted area, the name of the escort is captured in the DCAT ticket of the person under escort. |

### MA-2(2) - Automated Maintenance Activities

(a) Schedule, conduct, and document maintenance, repair, and replacement actions for the system using [Assignment: organization-defined automated mechanisms] ; and

(b) Produce up-to date, accurate, and complete records of all maintenance, repair, and replacement actions requested, scheduled, in process, and completed.

|  |
| --- |
| **MA-2(2) Control Summary Information** |
| Responsible Roles: Datacenter Hosting |
| Parameter ma-2.2\_prm\_1: organization-defined automated mechanisms |
| Parameter ma-02.02\_odp.01: |
| Parameter ma-02.02\_odp.02: |
| Parameter ma-02.02\_odp.03: |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **MA-2(2) What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for automating remote maintenance activities to schedule, conduct, and document remote maintenance and repairs of customer-deployed operating systems.  **Azure**  **Critical Environment Equipment**  Azure datacenters rely on a computerized maintenance management system to manage maintenance schedules and work order management.  **Site Services**  All Site Services work on Azure assets are scheduled, performed, documented, and reviewed in work tickets within the workflow ticketing tool. No work can occur without an approved work ticket. |
| **Part B**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for automating remote maintenance activities, including the production of up-to date, accurate, and complete records of all remote maintenance and repair actions requested, scheduled, in process, and completed for customer-deployed operating systems.  **Azure**  **Critical Environment Equipment**  The maintenance ticketing tracking tool is used to document and track all maintenance on CE equipment.  **Site Services**  All Site Services work on Azure assets are scheduled, performed, documented, and reviewed in work tickets within the workflow ticketing tool. |

## MA-3 Maintenance Tools

a. Approve, control, and monitor the use of system maintenance tools; and

b. Review previously approved system maintenance tools [at least annually].

|  |
| --- |
| **MA-3 Control Summary Information** |
| Responsible Roles: Datacenter Hosting |
| Parameter ma-3(b): at least annually |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **MA-3 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for approving, controlling and monitoring system maintenance tools used on customer-deployed operating systems.  **Azure**  All maintenance work must be approved prior to work beginning. Azure implements maintenance tools control by creating an access level within the Datacenter Access Tool (DCAT). Each facility contains a restricted physical lock box or access-controlled room for the storage of specialized maintenance tools, such as fluke ether scopes, fluke fiber channel testers, Ethernet toners, etc. Access is controlled to the lock box or storage room using the DCAT tool to prohibit unauthorized access to the maintenance tools. This ensures that only personnel with approved access can access the tools.  Third-party maintenance personnel may provide their own calibrated tools or assets where necessary. The same access controls in DCAT that limit access to the on-site tooling are also in place for all work areas where Critical Environment (CE) assets are present. Azure limits where any personnel can go and what doors they can open. To access the work site, they must follow CE procedural requirements.  The Site Services team performs routine inventory checks to verify the status of all tools. Access to lock box or maintenance storage room is tracked in the access smart card reader logs, which are available in the event of an investigation. On a quarterly basis, the datacenter management team and physical security teams perform audits of the DCAT access list to keep the access list of maintenance personnel current. Personnel terminations or transfers are reflected immediately through a manual update of the access list.  In addition, for logical access, maintenance is performed through the utilization of the SI, CM, AC, AU, and IR control families mentioned in this System Security Plan (SSP) document. Logical maintenance is performed through configuration management, access management, monitoring, and incident response tooling and processes. The tooling that are leveraged are ASM, SCUBA, Microsoft Entra ID (formerly AAD), JIT, build services, and incident response ticketing services. |
| **Part B**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for reviewing previously approved system maintenance tools at customer-defined frequency for customer-deployed resources.  **Azure**  The Site Services team performs routine inventory checks to verify the status of all tools. Access to lock box or maintenance storage room is tracked in the access smart card reader logs, which are available in the event of an investigation. On a quarterly basis, the datacenter management team and physical security teams perform audits of the DCAT access list to keep the access list of maintenance personnel current. Personnel terminations or transfers are reflected immediately through a manual update of the access list.  In addition, for logical access, maintenance is performed through the utilization of the SI, CM, AC, AU, and IR control families mentioned in this System Security Plan (SSP) document. Logical maintenance is performed through configuration management, access management, monitoring, and incident response tooling and processes. The tooling that are leveraged are ASM, SCUBA, Microsoft Entra ID (formerly AAD), JIT, build services, and incident response ticketing services. |

### MA-3(1) - Inspect Tools

Inspect the maintenance tools used by maintenance personnel for improper or unauthorized modifications.

|  |
| --- |
| **MA-3(1) Control Summary Information** |
| Responsible Roles: Datacenter Hosting |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **MA-3(1) What is the solution and how is it implemented?** |
| **Azure**  The Site Services team maintains an inventory of approved maintenance tools for use within the datacenter. Maintenance personnel are directed to use the provided maintenance tools. Datacenter Management (DCM) approval is required to use tools not provided by the datacenter. Physical hand tools such as screwdrivers, wrenches, etc., are exempt from this control. |

### MA-3(2) - Inspect Media

Check media containing diagnostic and test programs for malicious code before the media are used in the system.

|  |
| --- |
| **MA-3(2) Control Summary Information** |
| Responsible Roles: Datacenter Hosting |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **MA-3(2) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for checking media containing maintenance diagnostic and test programs for malicious code prior to deployment on customer-deployed operating systems.  **Azure**  Use of mobile computing or storage media is prohibited in the production environment of Azure datacenters without datacenter management approval. Use of personally owned media is prohibited from being used in the production environment of Azure datacenters.  Azure implements a process to inspect laptops and other mobile devices prior to being used in the production environment of Azure datacenters. The process requires that personnel from Site Services inspect laptops to validate that a full antivirus and anti-malware scan has been performed within twenty-four (24) hours of the datacenter visit, that the virus definition files are current, and that real-time scanning is configured. Laptops that have been validated are marked with an inspection sticker. Security officers are trained to challenge personnel using laptops in the production environment to verify that the laptops have undergone and passed inspection. |

### MA-3(3) - Prevent Unauthorized Removal

Prevent the removal of maintenance equipment containing organizational information by:

(a) Verifying that there is no organizational information contained on the equipment;

(b) Sanitizing or destroying the equipment;

(c) Retaining the equipment within the facility; or

(d) Obtaining an exemption from [the information owner] explicitly authorizing removal of the equipment from the facility.

|  |
| --- |
| **MA-3(3) Control Summary Information** |
| Responsible Roles: Datacenter Hosting |
| Parameter ma-03.03\_odp: Datacenter Management, Property asset owners |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **MA-3(3) What is the solution and how is it implemented?** |
| **Part A**  **Azure**  Maintenance tools are datacenter specific and are not removed and are retained within the facility. Each facility contains a restricted physical lock box or storage room that stores maintenance tools, such as fluke ether scopes, fluke fiber channel testers, Ethernet toners, etc. Access is controlled to the lock box or storage room in DCAT to prohibit unauthorized access to the maintenance tools. |
| **Part B**  **Azure**  Maintenance tools are datacenter specific and are not removed and are retained within the facility. Each facility contains a restricted physical lock box or storage room that stores maintenance tools, such as fluke ether scopes, fluke fiber channel testers, Ethernet toners, etc. Access is controlled to the lock box or storage room in DCAT to prohibit unauthorized access to the maintenance tools. |
| **Part C**  **Azure**  Maintenance tools are datacenter specific and are not removed and are retained within the facility. Each facility contains a restricted physical lock box or storage room that stores maintenance tools, such as fluke ether scopes, fluke fiber channel testers, Ethernet toners, etc. Access is controlled to the lock box or storage room in DCAT to prohibit unauthorized access to the maintenance tools. |
| **Part D**  **Azure**  Maintenance tools are datacenter specific and are not removed and are retained within the facility. Each facility contains a restricted physical lock box or storage room that stores maintenance tools, such as fluke ether scopes, fluke fiber channel testers, Ethernet toners, etc. Access is controlled to the lock box or storage room in DCAT to prohibit unauthorized access to the maintenance tools. |

## MA-4 Nonlocal Maintenance

a. Approve and monitor nonlocal maintenance and diagnostic activities;

b. Allow the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the system;

c. Employ strong authentication in the establishment of nonlocal maintenance and diagnostic sessions;

d. Maintain records for nonlocal maintenance and diagnostic activities; and

e. Terminate session and network connections when nonlocal maintenance is completed.

|  |
| --- |
| **MA-4 Control Summary Information** |
| Responsible Roles: JIT, OneIdentity, Azure Compliance, SDL, VPN, Jumpbox |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **MA-4 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for approving and monitoring of non-local maintenance and diagnostic activities on customer-deployed operating systems.  **Azure**  All access, including that for nonlocal maintenance, is approved per procedures via OneIdentity and JIT and changes are approved through the procedures. Azure adheres to the Microsoft Security Development Lifecycle (SDL) process, which requires all development teams to utilize standard approved tools and their associated security checks.  Azure authorizes, monitors, and controls nonlocal maintenance and diagnostic activities within the Azure managed network. All nonlocal network maintenance is performed via the change management process, which includes the approval of time-bound JIT requests specific to service team groups and the monitoring of actions taken at the asset and service level through the audit logging and monitoring pipeline. |
| **Part B**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for using maintenance and diagnostic tools that are consistent with organizational policy and documented in the security plan, when performing non-local maintenance on customer-deployed operating systems.  **Azure**  Nonlocal maintenance may be performed by authorized Azure personnel. Use of nonlocal maintenance and diagnostics tools are allowed within the Azure environment as long as the use is consistent with the configuration management processes. |
| **Part C**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for using strong authenticators when establishing non-local maintenance and diagnostic sessions on customer-deployed operating systems.  **Azure**  Azure enforces strong identification and authentication controls in conducting nonlocal maintenance and diagnostic activities. Authentication is handled by AD using Thales and Idemia smart cards. |
| **Part D**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for maintaining records for non-local maintenance and diagnostic activities on customer-deployed operating systems.  **Azure**  Auditing of maintenance and diagnostics within the Azure environment are performed via Azure DevOps and as part of the JIT elevation process. All nonlocal network maintenance must be documented in work tickets. Maintenance and diagnostic activities are logged in relevant logging and monitoring tool logs. |
| **Part E**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for terminating session and network connections when non-local maintenance is completed on customer-deployed operating systems.  **Azure**  Nonlocal sessions are terminated after the JIT elevation period expires. Nonlocal maintenance is performed via RDGWs, SSH, and SSL VPNs which enforce a network disconnect and allow users to terminate connections at the completion of the work. |

### MA-4(3) - Comparable Security and Sanitization

(a) Require that nonlocal maintenance and diagnostic services be performed from a system that implements a security capability comparable to the capability implemented on the system being serviced; or

(b) Remove the component to be serviced from the system prior to nonlocal maintenance or diagnostic services; sanitize the component (for organizational information); and after the service is performed, inspect and sanitize the component (for potentially malicious software) before reconnecting the component to the system.

|  |
| --- |
| **MA-4(3) Control Summary Information** |
| Responsible Roles: JIT, VPN, Jumpbox, Change Management, SAW |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **MA-4(3) What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for performing all non-local maintenance of customer-deployed operating systems from an information system that has comparable security.  **Azure**  Nonlocal maintenance and diagnostic services are performed by first logging in via RDP to a Jumpbox, Debug Server, or Network Hop Box from a Secure Administrative Workstation (SAW) machine on Microsoft CorpNet, and then initiating a second RDP session from the interim device to the destination target asset. No direct connection is possible from workstations to the destination asset. TLS 1.2/1.3 is used to protect RDP connections.  Azure requires strong identification and authentication for nonlocal maintenance and diagnostic sessions. Azure uses combinations of elevated access accounts and smart cards to access assets. When nonlocal maintenance is completed via RDGW or SSH or SSL VPN, the session is terminated by the user or is disconnected after fifteen (15) minutes of inactivity the information system.  All nonlocal network maintenance and diagnostic sessions are managed through configuration management process. Changes must be approved and documented in work tickets. Before changes are automatically deployed in the production environment there is a required quality control step that requires peer review of the proposed change, and a safe deployment process during deployment. After changes are implemented, there is a quality control process to review success criteria against logged work tickets from the past month. |
| **Part B**  **Azure**  Physical components within the Azure environment are not removed from the Azure datacenter for nonlocal maintenance. Digital media does not leave the secure physical Azure boundary of the colocation unless it is being taken for physical destruction by shredding onsite. |

## MA-5 Maintenance Personnel

a. Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel;

b. Verify that non-escorted personnel performing maintenance on the system possess the required access authorizations; and

c. Designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

|  |
| --- |
| **MA-5 Control Summary Information** |
| Responsible Roles: OneIdentity, Datacenter Hosting, CELA, Personnel Screening |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **MA-5 What is the solution and how is it implemented?** |
| **Part A**  **Azure**  Maintenance personnel authorization at Azure datacenters is managed through the DCAT system. All FTEs and vendors’ physical access to the datacenters is managed through DCAT. Logical access (any nonlocal maintenance) is managed through the CM process and access is documented, provisioned, and approved.  All maintenance work requires an associated work ticket. In order to physically access the datacenter to perform maintenance, the person must be approved by the Datacenter Management (DCM) team via a DCAT request. When arriving at the datacenter, a person’s identity is matched against their approved DCAT request. The DCAT tool manages the areas that maintenance personnel can access. The principle of least privilege is used in granting access. Azure datacenters have resident maintenance teams called Site Services and Critical Environment (CE) teams. On a quarterly basis, the datacenter management team and physical security teams perform audits of the DCAT access list to keep the access list of maintenance personnel current. Personnel terminations or transfers are reflected immediately through a manual update of the access list. |
| **Part B**  **Azure**  Maintenance personnel have their physical access authorizations managed in the DCAT system. Site Services and CE teams have certification requirements or equivalent tenure and training that ensure their team members are knowledgeable in supporting their respective datacenter environments. |
| **Part C**  **Azure**  Maintenance personnel with the appropriate technical competence and access authorizations escort any vendor that is required to perform maintenance on the system. |

### MA-5(1) - Individuals Without Appropriate Access

(a) Implement procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, that include the following requirements:

(1) Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified; and

(2) Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured; and

(b) Develop and implement [alternate controls to be developed and implemented in the event that a system component cannot be sanitized, removed, or disconnected from the system are defined;] in the event a system component cannot be sanitized, removed, or disconnected from the system.

|  |
| --- |
| **MA-5(1) Control Summary Information** |
| Responsible Roles: Datacenter Hosting, CELA, Personnel Screening |
| Parameter ma-05.01\_odp: alternate controls |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **MA-5(1) What is the solution and how is it implemented?** |
| **Part A1**  **Azure**  All visitors to datacenters who must gain physical access to perform maintenance must be approved by the Datacenter Management (DCM) team for access through a DCAT request . When arriving at the datacenter, a person’s identity is matched against their approved DCAT request. Additionally, visitors that do not have appropriate access approvals, such as maintenance vendors, are escorted by someone who possesses the technical competence and appropriate clearances and access to supervise the work they are performing. |
| **Part A2**  **Azure**  All visitors to datacenters who must gain physical access to perform maintenance must be approved by the Datacenter Management (DCM) team for access through a DCAT request . When arriving at the datacenter, a person’s identity is matched against their approved DCAT request. Additionally, visitors that do not have appropriate access approvals, such as maintenance vendors, are escorted by someone who possesses the technical competence and appropriate clearances and access to supervise the work they are performing. Visitors without access approvals or clearances are not permitted logical access to system assets. |
| **Part B**  **Azure**  If a data-bearing device (DBD) cannot be sanitized prior to necessary maintenance, it is destroyed to ensure the confidentiality of customer data. |

## MA-6 Timely Maintenance

Obtain maintenance support and/or spare parts for [system components for which maintenance support and/or spare parts are obtained are defined;] within [a timeframe to support advertised uptime and availability] of failure.

|  |
| --- |
| **MA-6 Control Summary Information** |
| Responsible Roles: Datacenter Hosting, BCDR |
| Parameter ma-06\_odp.01: Critical components list maintained in the maintenance tracking tool |
| Parameter ma-06\_odp.02: Spare parts or vendor agreements are acquired as needed to support the replacement SLAs |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **MA-6 What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for timely maintenance support of customer-deployed operating systems.  **Azure**  Azure datacenters maintain resident maintenance personnel as part of the Critical Environment (CE) team to support critical datacenter infrastructure systems as well as personnel as part of the Site Services team to support datacenter operations. The CE and Site Services teams have identified critical security and technology system components which they maintain spares for onsite. Critical systems are designed in N+1 configurations and services are designed to be resilient. This allows the datacenter management team to meet recovery goals in the event of a service interruption or contingency plan situation. Critical information system services are provisioned from more than one datacenter to prevent an interruption in service due to an incident at one of the datacenters. Services are responsible for deploying to multiple datacenters to provide for redundancy and resiliency. |

# Media Protection (MP)

## MP-1 Policy and Procedures

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (OneOrMore): organization-level;mission/business process-level;system-level] media protection policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the media protection policy and the associated media protection controls;

b. Designate an [an official to manage the media protection policy and procedures is defined;] to manage the development, documentation, and dissemination of the media protection policy and procedures; and

c. Review and update the current media protection:

1. Policy [at least annually] and following [events that would require the current media protection policy to be reviewed and updated are defined;] ; and

2. Procedures [at least annually] and following [significant changes].

|  |
| --- |
| **MP-1 Control Summary Information** |
| Responsible Roles: SOP Team, Policy |
| Parameter mp-1(a): all personnel |
| Parameter mp-01\_odp.01: |
| Parameter mp-01\_odp.02: |
| Parameter mp-01\_odp.03: a Microsoft-wide |
| Parameter mp-01\_odp.04: the Microsoft Information Risk Management Council (IRMC) organization |
| Parameter mp-01\_odp.05: at least annually |
| Parameter mp-01\_odp.06: significant changes |
| Parameter mp-01\_odp.07: at least annually |
| Parameter mp-01\_odp.08: significant changes |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☒ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **MP-1 What is the solution and how is it implemented?** |
| **Part A1**  **Customer Responsibility**  The customer is responsible for developing, documenting, and disseminating media protection policy and procedures that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Due to there not being any customer-controlled media within the scope of systems deployed on Azure, all media protection controls will be implemented and managed by Azure. However, the customer is still responsible for the appropriate policy and procedure documents.  **Azure**  Azure addresses the media protection policy as part of the Microsoft security policies, of which there are two sets: the Microsoft Security Policy (MSP) that is applicable to all Microsoft personnel and the Microsoft Security Program Policy (MSPP), which is applicable to all Microsoft personnel that have a responsibility for security. The Microsoft Information Risk Management Council (IRMC) is the governance body with review and approval responsibility for the MSP and MSPP. Within Azure, the MSPP specifically applies to all Microsoft personnel with security objectives such as designing, building, and operating Azure and across all information and processes used in the conduct of Microsoft business. All Azure personnel are accountable and responsible for complying with these guiding principles within their designated roles. The policy addresses the following:  \* How important organizational records relating to the organization’s Information Security Program, independent of media type, must be retained, stored, protected, and, if appropriate, destroyed according to the established information handling procedures for the records  Additionally, the policy addresses the purpose, scope, roles, responsibilities, compliance requirements, and required coordination among the various Microsoft organizations that provide some level of support to all services. The policies indicate Microsoft management’s commitment and are a component of the risk management strategy which provides Azure personnel with a current set of clear and concise information security requirements.  The MSP is available to all Microsoft personnel on the Microsoft Policy website on the Microsoft intranet, and the MSPP and Security Standards are available through the Liquid tool, also on the Microsoft intranet. The Azure SOPs are stored in the Azure Security, Privacy & Compliance SharePoint site. This SharePoint site is accessible to all Azure personnel.  Service teams may supplement the Azure policies and procedures with offering-specific policies and procedures. Service-team-specific policies and procedures associated with media protection are documented and stored within internal Azure SharePoint sites. Only personnel with authorized credentials, adequate levels of permission, legitimate need to know, and specific roles and responsibilities are given access to the service-team-specific policies or procedures. |
| **Part A2**  **Customer Responsibility**  The customer is responsible for procedures to facilitate the implementation of the media protection policy and the associated media protection controls.  **Azure**  The Microsoft Asset Classification Standard and Asset Protection Standard implements the media protection policy and associated controls and documents the following procedures:  \* Handling and protection of assets  \* Asset classification  Service teams may supplement the Azure policies and procedures with offering-specific policies and procedures. Service-team-specific policies and procedures associated with media protection are documented and stored within internal Azure SharePoint sites. Only personnel with authorized credentials, adequate levels of permission, legitimate need to know, and specific roles and responsibilities are given access to the service-team-specific policies or procedures. |
| **Part B**  **Customer Responsibility**  The customer is responsible for designating an official to manage the development, documentation, and dissemination of media protection policy and procedures.  **Azure**  The Microsoft Information Risk Management Council (IRMC) organization is the governance body with approval responsibility for the Microsoft Security Policy (MSP) and Microsoft Security Program Policy (MSPP). The IRMC consists of representatives from security and risk management teams across Microsoft including Core Services Engineering and Operations (CSEO), Azure, and Global Security. The Customer Security and Trust: Security Engineering (CST-SE) organization manages the review and approval process and maintains the policies.  On an annual basis, the CST-SE conducts a line-by-line review of the MSP and MSPP. The Microsoft Security Policy (MSP) and Microsoft Security Program Policy (MSPP) Governance document describes each member’s role, types and frequency of review, escalation paths, approval process, and formal publishing procedures of the security policy. Throughout the year, if necessary, CST-SE may convene with the IRMC to conduct reviews after a significant review or change request. The approved policy update is published within the relevant tool on the Microsoft intranet. If service teams establish service-specific or team-specific policies, the respective service teams update the necessary policies at least annually. |
| **Part C1**  **Customer Responsibility**  The customer is responsible for reviewing and updating the current media protection policy on a regular basis and following organization defined events.  **Azure**  The Azure team updates the Azure SOPs at least annually through a formal review process. If needed, the Azure team updates the SOP after a significant change affecting policy execution as well. If established, service-team-specific procedures are updated by their respective teams. The individual service teams review and update their respective SOPs at least annually and when required by a significant change. |
| **Part C2**  **Customer Responsibility**  The customer is responsible for reviewing and updating the current media protection procedures on a regular basis and following organization defined events.  **Azure**  The Azure team updates the Azure SOPs at least annually through a formal review process. If needed, the Azure team updates the SOP after a significant change affecting policy execution as well. If established, service-team-specific procedures are updated by their respective teams. The individual service teams review and update their respective SOPs at least annually and when required by a significant change. |

## MP-2 Media Access

Restrict access to [all types of digital and/or non-digital media containing sensitive information] to [Assignment: organization-defined personnel or roles].

|  |
| --- |
| **MP-2 Control Summary Information** |
| Responsible Roles: OneIdentity, Datacenter Hosting |
| Parameter mp-2-1: All media |
| Parameter mp-2-2: Personnel with a legitimate business purpose |
| Parameter mp-02\_odp.01: |
| Parameter mp-02\_odp.02: |
| Parameter mp-02\_odp.03: |
| Parameter mp-02\_odp.04: |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **MP-2 What is the solution and how is it implemented?** |
| **Azure**  Azure has restricted media access through the implementation of the Microsoft Security Program Policy (MSPP). Logical access to digital media is controlled via Active Directory Group Policy Objects (AD GPOs) and security groups in OneIdentity. Physical access to all media is restricted by the datacenter access process. Access is restricted to individuals who have a legitimate business purpose for accessing the data. The Asset Protection Standard defines the safeguards required to protect the confidentiality, integrity, and availability of information assets within Azure datacenters. Azure considers digital media for this control to be the server and network device assets secured at Azure datacenters. Non-digital media is not used for storage of Azure information. |

## MP-3 Media Marking

a. Mark system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and

b. Exempt [no removable media types] from marking if the media remain within [organization-defined security safeguards not applicable].

(b) Guidance: Second parameter not-applicable

|  |
| --- |
| **MP-3 Control Summary Information** |
| Responsible Roles: Datacenter Hosting |
| Parameter mp-03\_odp.01: No removable media types |
| Parameter mp-03\_odp.02: Not applicable |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **MP-3 What is the solution and how is it implemented?** |
| **Part A**  **Azure**  Assets within Azure datacenters are classified with a High, Moderate, or Low Business Impact (HBI, MBI, LBI) designation which requires different levels of security and handling precautions. Asset owners are required to classify their assets. HBI assets are secured in a rack with small, red placard labeled HBI on the door of the rack. |
| **Part B**  **Azure**  Asset owners are required to assign their assets an asset classification and no assets are exempt from this requirement. In the Azure datacenter environment, assets refer to servers, network devices, and magnetic tapes. Non-digital media is not used in the datacenters.  Azure implements maintenance tools control by creating an access level within the Datacenter Access Tool (DCAT). Each facility contains a restricted physical lock box or access-controlled room for the storage of specialized maintenance tools, such as fluke ether scopes, fluke fiber channel testers, ethernet toners, and USBs. Access is controlled to the lock box or storage room using the DCAT tool to prohibit unauthorized access to the maintenance tools. This ensures that only personnel with approved access can access the tools.  Third-party maintenance personnel may provide their own calibrated tools or assets where necessary. The same access controls in DCAT that limit access to the on-site tooling are also in place for all work areas where Critical Environment (CE) assets are present. Azure limits where any personnel can go and what doors they can open. To access the work site, they must follow CE procedural requirements.  The Site Services team performs routine inventory checks to verify the status of all tools. Access to lock box or maintenance storage room is tracked in the access smart card reader logs, which are available in the event of an investigation. On a quarterly basis, the datacenter management team and physical security teams perform audits of the DCAT access list to keep the access list of maintenance personnel current. Personnel terminations or transfers are reflected immediately through a manual update of the access list. |

## MP-4 Media Storage

a. Physically control and securely store [all types of digital and non-digital media with sensitive information] within [see additional FedRAMP requirements and guidance] ; and

b. Protect system media types defined in MP-4a until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

(a) Requirement: The service provider defines controlled areas within facilities where the information and information system reside.

|  |
| --- |
| **MP-4 Control Summary Information** |
| Responsible Roles: Datacenter Hosting |
| Parameter mp-4(a)-1: digital media assets as documented in the inventory |
| Parameter mp-4(a)-2: facility-specific controlled areas |
| Parameter mp-04\_odp.01: |
| Parameter mp-04\_odp.02: |
| Parameter mp-04\_odp.03: |
| Parameter mp-04\_odp.04: |
| Parameter mp-04\_odp.05: |
| Parameter mp-04\_odp.06: |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **MP-4 What is the solution and how is it implemented?** |
| **Part A**  **Azure**  Azure digital media assets are physically and securely stored within Azure datacenters, colocation rooms, or Global Cloud Collaboration Centers (GC3s). Azure locations have multiple layers of physical access controls and video surveillance in place to provide secure storage. Digital media includes servers, network devices, and magnetic tapes. Non-digital media is not used by Azure in the datacenter environment. Facilities define controlled areas as appropriate for their footprint and layout. Any areas containing digital media assets are considered controlled regardless of facility layout and are protected by the physical and environmental controls. |
| **Part B**  **Azure**  Azure digital media assets are protected in Azure datacenters and GC3s through physical access controls and logical access controls for the lifetime of the asset. Azure assets are cleared, purged, or destroyed with methods NIST Special Publication 800-88 Revision 1 prior to the asset’s reuse or disposal. Azure utilizes data erasure units from Blancco. Blancco supports NIST Special Publication 800-88 Revision 1 requirements for cleansing and purging/secure erasure. For asset destruction, Azure utilizes onsite asset destruction services. |

## MP-5 Media Transport

a. Protect and control [all media with sensitive information] during transport outside of controlled areas using [prior to leaving secure/controlled environment: for digital media, encryption in compliance with Federal requirements and utilizes FIPS validated or NSA approved cryptography (see SC-13.); for non-digital media, secured in locked container];

b. Maintain accountability for system media during transport outside of controlled areas;

c. Document activities associated with the transport of system media; and

d. Restrict the activities associated with the transport of system media to authorized personnel.

(a) Requirement: The service provider defines security measures to protect digital and non-digital media in transport. The security measures are approved and accepted by the JAB/AO.

|  |
| --- |
| **MP-5 Control Summary Information** |
| Responsible Roles: Datacenter Hosting |
| Parameter mp-5(a): SafeNet KeySecure to manage cryptographic keys using a Federal Information Processing Standards (FIPS) 140-2 Level 3 validated encryption module and HSM to secure AES 256-bit encrypted data on the magnetic tapes |
| Parameter mp-05\_odp.01: digital media assets |
| Parameter mp-05\_odp.02: |
| Parameter mp-05\_odp.03: |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **MP-5 What is the solution and how is it implemented?** |
| **Part A**  **Azure**  Digital media at Azure datacenters consist of servers, network devices, and magnetic tapes. Azure datacenters do not use non-digital media. Azure utilizes secure transport and data deletion to protect media that is being transported outside the datacenter.  All media being transported from Azure datacenters require accurate tracking. Tickets are created to arrange and track the transportation of media. Azure has contracted with several approved vendors to provide secure shipping services. Secure Transport begins with an accurate inventory and chain of custody. Authorized asset managers are required to manage the exchange of assets. Assets are inventoried at the time of delivery to the transporter. Requirements for transporting an asset are defined according to their asset classification and data classification. If data is required to be intact, an approved policy exception request is required. The asset manager must witness the container being locked and a tamper proof seal applied. Secure Transport could have additional requirements such as a dedicated transport for only Microsoft assets, GPS tracking, and only stopping at Microsoft locations. In cases of longer transport routes, the requirement could be that there are multiple drivers and trucks with sleeping quarters to provide for non-stop delivery. At the delivery location, the transport company’s approved personnel must be present to witness the removal of the tamper proof seal and unlocking of the container. The receiving personnel inventories the shipment and send a message confirming the receipt of the assets. This inventory is validated by the Microsoft asset manager.  Azure contracts with a vendor to provide equipment destruction. All assets are required to be destroyed onsite. Azure assets are cleansed/purged with methods consistent with NIST Special Publication 800-88 Revision 1 prior to reuse. Prior to cleansing or destruction, an inventory is created by Datacenter Logistics. If a vendor is used for destruction, the vendor provides a certificate of destruction for each asset destroyed, which is validated by the asset manager. |
| **Part B**  **Azure**  Azure maintains accountability for assets leaving the datacenter consistent with NIST Special Publication 800-88 Revision 1: consistent cleansing/purging, asset destruction, encryption, accurate inventorying, tracking, and protection of chain of custody during transport. |
| **Part C**  **Azure**  Azure restricts the activities of asset transport to authorized personnel through the protection of the chain of custody. The use of locks, tamper proof seals, and requiring validation of the asset inventories ensures that only authorized personnel are involved in the asset transport. |
| **Part D**  **Azure**  The transport of Azure digital media outside of the Azure security-controlled space requires the supervision of two Datacenter Operations (DCOPs) team members. The assets are accompanied and supervised at all times by authorized personnel until they are destroyed. The DPS team utilizes Iron Mountain and Azure Cool Storage for storage of media for media that contains valid, unexpired data. |

## MP-6 Media Sanitization

a. Sanitize [techniques and procedures IAW NIST SP 800-88 Section 4: Reuse and Disposal of Storage Media and Hardware] prior to disposal, release out of organizational control, or release for reuse using [Assignment: organization-defined sanitization techniques and procedures] ; and

b. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

|  |
| --- |
| **MP-6 Control Summary Information** |
| Responsible Roles: Datacenter Hosting |
| Parameter mp-6(a)-1: all media |
| Parameter mp-6(a)-2: techniques depending on media type; for digital media, overwrite at least three (3) times; non-digital media via secure shredding |
| Parameter mp-06\_odp.01: |
| Parameter mp-06\_odp.02: |
| Parameter mp-06\_odp.03: |
| Parameter mp-06\_odp.04: |
| Parameter mp-06\_odp.05: |
| Parameter mp-06\_odp.06: |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **MP-6 What is the solution and how is it implemented?** |
| **Part A**  **Azure**  In Azure datacenters , Azure digital media is sanitized using approved tools and in compliance with customer requirements, including NIST Special Publication 800-88 Revision 1 prior to being reused. Non-digital media is not used by Azure in the datacenter environment.  All data bearing devices (DBDs) used by Azure are shredded by an approved ITAD Vendor or customer per customer standards on site. No DBDs leave the Azure datacenters . If hardware is considered volatile and deemed returnable to the supplier, it is shipped out via the standard RMA process as outlined in the Sparing and RMA Strategy. |
| **Part B**  **Azure**  Azure uses data erasure units and processes to sanitize data in compliance with customer requirements , including NIST Special Publication 800-88 Revision 1 which are commensurate with the Azure asset classification of the asset. For assets requiring destruction, Azure utilizes onsite asset destruction services. |

### MP-6(1) - Review, Approve, Track, Document, and Verify

Review, approve, track, document, and verify media sanitization and disposal actions.

Requirement: Must comply with NIST SP 800-88

|  |
| --- |
| **MP-6(1) Control Summary Information** |
| Responsible Roles: Datacenter Hosting |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **MP-6(1) What is the solution and how is it implemented?** |
| **Azure**  Digital media at Azure datacenters hosting the Azure environment consist of servers, network devices, and physical hard disks. Azure datacenters do not use non-digital media.  Digital media within Azure is not allowed to be transported from the Azure location unless it is being destroyed. Assets that are to be destroyed are stored in locked storage bins. At the time of destruction and under CCTV supervision, Azure digital media is removed from the locked storage bin and scanned to log the serial number of the asset to be destroyed. The asset is shredded while being supervised by cleared personnel. The destruction vendor issues a certificate of destruction for the assets that were destroyed. |

### MP-6(2) - Equipment Testing

Test sanitization equipment and procedures [at least every six (6) months] to ensure that the intended sanitization is being achieved.

Guidance: Equipment and procedures may be tested or validated for effectiveness

|  |
| --- |
| **MP-6(2) Control Summary Information** |
| Responsible Roles: Datacenter Hosting |
| Parameter mp-6.2\_prm\_1: at least every one hundred and eighty (180) days |
| Parameter mp-06.02\_odp.01: |
| Parameter mp-06.02\_odp.02: |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **MP-6(2) What is the solution and how is it implemented?** |
| **Azure**  Azure uses data erasure units and processes to sanitize data in compliance with NIST Special Publication 800-88 Revision 1 prior to being reused. Every one hundred and eighty (180) days, the Microsoft Security Response Center (MSRC) working in the Cyber Defense Operations Center (CDOC) tests the Azure data erasure units and the process for erasure. In the test, Cloud Operations + Innovation Engineering (CO + IE) verifies that the intended sanitization is being achieved through a forensic analysis of tested hard drives to confirm that the data has been sanitized by the data erasure units. |

### MP-6(3) - Nondestructive Techniques

Apply nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the system under the following circumstances: [circumstances requiring sanitization of portable storage devices are defined;].

Requirement: Must comply with NIST SP 800-88

|  |
| --- |
| **MP-6(3) Control Summary Information** |
| Responsible Roles: Datacenter Hosting |
| Parameter mp-06.03\_odp: before use in Azure |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **MP-6(3) What is the solution and how is it implemented?** |
| **Azure**  To prevent the infection of Azure by viruses or malware on portable storage devices, Azure datacenters follow the Tools and Removable Media Security Procedure in the Datacenter Services Run Book. The procedure specifies that the following actions be taken with USB drives before use in the Azure environment:  \* Format the USB drives when the drives are first purchased from the manufacturer or vendor, before the initial use or when being reused for a different tool.  \* Scan any USB drive to be used in an Azure-designated area for viruses and malware, before taking the drive into the area.  \* After using a drive within an Azure-designated area, format the drive before leaving the area.  The Tools and Removable Media Security Procedure also requires that all lost, discarded, stolen or misplaced thumb drives never be re-introduced into Azure, but that they be instead cataloged and destroyed. |

## MP-7 Media Use

a. [Selection: restrict;prohibit] the use of [types of system media to be restricted or prohibited from use on systems or system components are defined;] on [systems or system components on which the use of specific types of system media to be restricted or prohibited are defined;] using [controls to restrict or prohibit the use of specific types of system media on systems or system components are defined;] ; and

b. Prohibit the use of portable storage devices in organizational systems when such devices have no identifiable owner.

|  |
| --- |
| **MP-7 Control Summary Information** |
| Responsible Roles: Datacenter Hosting |
| Parameter mp-07\_odp.01: Defined information system media |
| Parameter mp-07\_odp.02: Prohibits |
| Parameter mp-07\_odp.03: All information systems |
| Parameter mp-07\_odp.04: Defined security safeguards |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **MP-7 What is the solution and how is it implemented?** |
| **Part A**  **Azure**  Asset owners are required to assign their assets with an asset classification and no assets are exempt from this requirement. In the Azure datacenters and GC3s, assets refer to servers and network devices. Other digital media like USB flash/thumb drives or CDs/DVDs are managed by specific policies and procedures, including the Asset Management section of the Microsoft Security Program Policy (MSPP), governing how those devices are managed. Non-digital media is not used. The usage of digital media in Azure datacenters and GC3s is monitored twenty-four (24) hours a day, seven (7) days a week via CCTV coverage. |
| **Part B**  **Azure**  Asset owners are required to assign their assets with an asset classification and no assets are exempt from this requirement. In the Azure datacenters and GC3s, assets refer to servers and network devices. All assets has identified owners and there are no assets left without identified owner. Other digital media like USB flash/thumb drives or CDs/DVDs are managed by specific policies and procedures, including the Asset Management section of the Microsoft Security Program Policy (MSPP), governing how those devices are managed. Non-digital media is not used. The usage of digital media in Azure datacenters and GC3s is monitored twenty-four (24) hours a day, seven (7) days a week via CCTV coverage. |

# Physical and Environmental Protection (PE)

## PE-1 Policy and Procedures

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (OneOrMore): organization-level;mission/business process-level;system-level] physical and environmental protection policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the physical and environmental protection policy and the associated physical and environmental protection controls;

b. Designate an [an official to manage the physical and environmental protection policy and procedures is defined;] to manage the development, documentation, and dissemination of the physical and environmental protection policy and procedures; and

c. Review and update the current physical and environmental protection:

1. Policy [at least annually] and following [events that would require the current physical and environmental protection policy to be reviewed and updated are defined;] ; and

2. Procedures [at least annually] and following [significant changes].

|  |
| --- |
| **PE-1 Control Summary Information** |
| Responsible Roles: SOP Team, Policy |
| Parameter pe-1(a): all personnel |
| Parameter pe-01\_odp.01: |
| Parameter pe-01\_odp.02: |
| Parameter pe-01\_odp.03: a Microsoft-wide |
| Parameter pe-01\_odp.04: the Microsoft Information Risk Management Council (IRMC) organization |
| Parameter pe-01\_odp.05: at least annually |
| Parameter pe-01\_odp.06: significant changes |
| Parameter pe-01\_odp.07: at least annually |
| Parameter pe-01\_odp.08: significant changes |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☒ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **PE-1 What is the solution and how is it implemented?** |
| **Part A1**  **Customer Responsibility**  The customer is responsible for developing, documenting, and disseminating physical and environmental protection policy and procedures that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Due to customers not having physical access to any resources in Azure datacenters, all physical and environmental protection controls will be implemented and managed by Azure. However, the customer is still responsible for the appropriate policy and procedure documents.  **Azure**  Azure addresses the physical and environmental protection policy as part of the Microsoft security policies, of which there are two sets: the Microsoft Security Policy (MSP) that is applicable to all Microsoft personnel, and the Microsoft Security Program Policy (MSPP), which is applicable to all Microsoft personnel that have a responsibility for security. The Microsoft Information Risk Management Council (IRMC) is the governance body with review and approval responsibility for the MSP and MSPP. Within Azure, the MSPP specifically applies to all Microsoft personnel with security objectives such as designing, building, and operating Azure and across all information and processes used in the conduct of Microsoft business. All Azure personnel are accountable and responsible for complying with these guiding principles within their designated roles. The policy addresses the following:  \* Prevention of unauthorized access, damage, or interference to Microsoft facilities  Additionally, the policy addresses the purpose, scope, roles, responsibilities, compliance requirements, and required coordination among the various Microsoft organizations that provide some level of support to all services. The policies indicate Microsoft management’s commitment and are a component of the risk management strategy which provides Azure personnel with a current set of clear and concise information security requirements.  The MSP is available to all Microsoft personnel on the Microsoft Policy website on the Microsoft intranet, and the MSPP and Security Standards are available through the Liquid tool, also on the Microsoft intranet. The Azure SOPs are stored in the Azure Security, Privacy & Compliance SharePoint site. This SharePoint site is accessible to all Azure personnel.  Service teams may supplement the Azure policies and procedures with offering-specific policies and procedures. Service-team-specific policies and procedures associated with physical and environmental protection are documented and stored within internal Azure SharePoint sites. Only personnel with authorized credentials, adequate levels of permission, legitimate need to know, and specific roles and responsibilities are given access to the service-team-specific policies or procedures. |
| **Part A2**  **Customer Responsibility**  The customer is responsible for procedures to facilitate the implementation of the physical and environmental protection policy and the associated physical and environmental protection controls.  **Azure**  The Physical and Environmental Security Standard implements the physical and environmental protection policy and associated controls and documents the following procedures:  \* Physical access control  \* Cyber Defense Operations (CDOC) operations  \* Audit and compliance  \* Technology, applications, and equipment employed at the datacenters  Service teams may supplement the Azure policies and procedures with offering-specific policies and procedures. Service-team-specific policies and procedures associated with physical and environmental protection are documented and stored within internal Azure SharePoint sites. Only personnel with authorized credentials, adequate levels of permission, legitimate need to know, and specific roles and responsibilities are given access to the service-team-specific policies or procedures. |
| **Part B**  **Customer Responsibility**  The customer is responsible for designating an official to manage the development, documentation, and dissemination of physical and environmental protection policy and procedures.  **Azure**  The Microsoft Information Risk Management Council (IRMC) organization is the governance body with approval responsibility for the Microsoft Security Policy (MSP) and Microsoft Security Program Policy (MSPP). The IRMC consists of representatives from security and risk management teams across Microsoft including Core Services Engineering and Operations (CSEO), Azure, and Global Security. The Customer Security and Trust: Security Engineering (CST-SE) organization manages the review and approval process and maintains the policies.  On an annual basis, the CST-SE conducts a line-by-line review of the MSP and MSPP. The Microsoft Security Policy (MSP) and Microsoft Security Program Policy (MSPP) Governance document describes each member’s role, types and frequency of review, escalation paths, approval process, and formal publishing procedures of the security policy. Throughout the year, if necessary, CST-SE may convene with the IRMC to conduct reviews after a significant review or change request. The approved policy update is published within the relevant tool on the Microsoft intranet. If service teams establish service-specific or team-specific policies, the respective service teams update the necessary policies at least annually. |
| **Part C1**  **Customer Responsibility**  The customer is responsible for reviewing and updating the current physical and environmental protection policy on a regular basis and following organization defined events.  **Azure**  The Azure team updates the Azure SOPs at least annually through a formal review process. If needed, the Azure team updates the SOP after a significant change affecting policy execution as well. If established, service-team-specific procedures are updated by their respective teams. The individual service teams review and update their respective SOPs at least annually and when required by a significant change. |
| **Part C2**  **Customer Responsibility**  The customer is responsible for reviewing and updating the current physical and environmental protection procedures on a regular basis and following organization defined events.  **Azure**  The Azure team updates the Azure SOPs at least annually through a formal review process. If needed, the Azure team updates the SOP after a significant change affecting policy execution as well. If established, service-team-specific procedures are updated by their respective teams. The individual service teams review and update their respective SOPs at least annually and when required by a significant change. |

## PE-2 Physical Access Authorizations

a. Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides;

b. Issue authorization credentials for facility access;

c. Review the access list detailing authorized facility access by individuals [at least every ninety (90) days] ; and

d. Remove individuals from the facility access list when access is no longer required.

|  |
| --- |
| **PE-2 Control Summary Information** |
| Responsible Roles: Datacenter Hosting |
| Parameter pe-2(c): at least every ninety (90) days |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **PE-2 What is the solution and how is it implemented?** |
| **Part A**  **Azure**  Access to an Azure datacenter must be approved by the Datacenter Management (DCM) team through the Datacenter Access Tool (DCAT). On a quarterly basis, the DCM team for each datacenter is required to perform an appropriateness review of the personnel with authorized access to their datacenter. The review consists of reviewing reports from security showing personnel with current access to the datacenter. The DCM determines the access changes to be made and communicates a request to security to have the changes performed. After the changes have been made, the DCM team reviews reports verifying that the changes have been completed. The quarterly access review is documented in a work ticket that includes the reports that were reviewed by the DCM team. These tickets are reviewed as part of quality control, quality assurance process. The DC Quarterly Access Review process is documented in the Datacenter Services (DCS) Standard Operating Procedure (SOP). In between quarterly access reviews, DCAT supports the least privilege principle by requiring access assignments to require an end date. After the end date is reached, access is removed by DCAT. The DCAT termination process can be manual or automatic. Manual scenarios are where a Datacenter Manager or security team member initiates the termination of an individual’s DCAT requests. An automatic termination occurs when an individual with a Microsoft alias/domain account has their employment terminated in Microsoft’s headcount management tool (Employee Central). Additionally, when access is no longer required, it is the standard procedure for security officers at the datacenter or the DCM team to manually request the termination of access. The DC Quarterly Access Review is a quarterly true-up of the access list and not the primary control relied upon to keep the access list current.  **Azure Third-Party (Leased) Datacenters**  The DCM of a leased datacenter is responsible for conducting the same access review as a fully-managed Azure datacenter. Instead of reviewing the access levels for the entire datacenter, the DCM requests the access list for the Microsoft areas from the datacenter's security team. The DCM is responsible for ensuring that both the landlord's access system and DCAT reflect the same data. The quarterly access review is conducted in the same manner as a fully-managed Azure datacenter.  DCAT requests are used in leased datacenter locations in a slightly different manner from a fully-managed Azure datacenter. The exception is that the approved DCAT request is emailed by the DCM team to the security team at the leased datacenter. The leased datacenter security team inputs the approved request into the leased datacenter's access tool. |
| **Part B**  **Azure**  DCAT is the authoritative source listing all personnel with authorized access to a specific datacenter. DCAT is linked with the datacenter’s physical security access control devices and authorizes access based on access levels that are approved by the DCM team. Access levels are assigned in DCAT to either a user’s Microsoft issued smart card or a temporary access smart card that is assigned at the datacenter by the Control Room Supervisor (CRS). Access levels are approved by the DCM team. Besides credentials assigned to physical smart cards, some areas of datacenter require two- factor authentication employing the user’s biometric data (hand geometry or fingerprint) as well as smart card authentication to gain authorized entry.  **Azure Third-Party (Leased) Datacenters**  At a leased datacenter, DCAT is still considered the authoritative source for access to Microsoft areas within the datacenter. All access request approvals are first processed in DCAT and then emailed to the leased datacenter's security team. The leased datacenter's security team only authorizes access to Microsoft areas to individuals with an approved DCAT request. Besides credentials assigned to physical smart cards, some areas of datacenter require two- factor authentication employing the user’s biometric data (hand geometry or fingerprint) as well as smart card authentication to gain authorized entry. |
| **Part C**  **Azure**  The physical security team and datacenter management team conducts a quarterly access review of the access control list to remove or update individual access as necessary. Terminations are handled immediately through the DCAT termination process. If termination of access to the datacenter is required, the DCM team provides the physical security team notification of termination request. Once processed, the DCM team verifies access has been terminated in DCAT.  Additionally, the DCAT system performs real time comparisons of access authorization and automatically removes access when access tickets expire. A person with an expired access ticket is escorted back to Security Operations Center to have their access renewed.  **Azure Third-Party (Leased) Datacenters**  The DCM of a leased datacenter is responsible for conducting the same access review as a fully-managed Azure datacenter. Instead of reviewing the access levels for the entire datacenter, the DCM requests the access list for the Microsoft areas from the datacenter's security team. The DCM is responsible for ensuring that both the landlord's access system and DCAT reflect the same data. The quarterly access review is conducted in the same manner as a fully-managed Azure datacenter.  DCAT requests are used as leased datacenters in a slightly different manner from a fully-managed Azure datacenter. The exception is that the approved DCAT request is emailed by the DCM team to the security team at the leased datacenter. The leased datacenter security team inputs the approved request into the leased datacenter's access tool. Terminations are handled immediately through the DCAT termination process and communication to the leased datacenter's security team. |
| **Part D**  **Azure**  The physical security team and DCM team conduct a quarterly review of the access control list to remove or update individual access as necessary. Terminations are handled immediately through a DCAT termination process detailed in Part c above. |

## PE-3 Physical Access Control

a. Enforce physical access authorizations at [entry and exit points to the facility in which the system resides are defined;] by:

1. Verifying individual access authorizations before granting access to the facility; and

2. Controlling ingress and egress to the facility using [Selection (OneOrMore): [physical access control systems or devices used to control ingress and egress to the facility are defined (if selected);] ;guards] ;

b. Maintain physical access audit logs for [entry or exit points for which physical access logs are maintained are defined;];

c. Control access to areas within the facility designated as publicly accessible by implementing the following controls: [physical access controls to control access to areas within the facility designated as publicly accessible are defined;];

d. Escort visitors and control visitor activity [in all circumstances within restricted access area where the information system resides];

e. Secure keys, combinations, and other physical access devices;

f. Inventory [physical access devices to be inventoried are defined;] every [at least annually] ; and

g. Change combinations and keys [at least annually or earlier as required by a security relevant event.] and/or when keys are lost, combinations are compromised, or when individuals possessing the keys or combinations are transferred or terminated.

|  |
| --- |
| **PE-3 Control Summary Information** |
| Responsible Roles: Datacenter Hosting |
| Parameter pe-3(g): at least annually or earlier as required by a security relevant event |
| Parameter pe-03\_odp.01: all physical access points to the facility |
| Parameter pe-03\_odp.02: CSP defined physical access control systems/devices and guards |
| Parameter pe-03\_odp.03: |
| Parameter pe-03\_odp.04: all physical access points to the facility |
| Parameter pe-03\_odp.05: guards during working hours; guards, locks, and/or alarms during non-working hours |
| Parameter pe-03\_odp.06: at all times while in the datacenter |
| Parameter pe-03\_odp.07: keys, temporary access badges, access badge readers, and similar devices |
| Parameter pe-03\_odp.08: at least annually |
| Parameter pe-03\_odp.09: |
| Parameter pe-03\_odp.10: |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **PE-3 What is the solution and how is it implemented?** |
| **Part A1**  **Azure**  Azure enforces physical access authorizations for all physical access points to Azure datacenters. The exteriors of the datacenter buildings are non-descript and do not advertise that they are Microsoft datacenters.  Depending on the design of a datacenter, physical access authorizations at Azure datacenters may begin at a controlled perimeter gate or secured facility door that requires either access smart card authorization or security officer authorization.  Main access to Azure datacenter facilities is restricted to a single point of entry that is manned twenty-four (24) hours a day, seven (7) days a week by security personnel. Emergency exits are alarmed and under video surveillance. Electronic access control devices are installed on doors separating the reception area from the facilities’ interior to restrict access to approved personnel only. Azure datacenters have a security operations desk located in the reception area and in line of sight of the single entry point. The datacenter lobbies have man-trap portal devices that require multifactor authentication such as access card and biometric hand geometry or fingerprint authentication to pass beyond the lobby. Areas within Microsoft datacenters that contain critical systems (e.g., colocations, critical environments, Main Distribution Frame (MDF) rooms, etc.) are further restricted through various security mechanisms such as electronic access control, biometric devices, and anti-passback controls. Additionally, doors are alarmed and under video surveillance.  Access authorizations at Azure datacenters are managed through the Datacenter Access Tool (DCAT). DCAT contains the authorized access lists of personnel who have been approved by the Datacenter Management (DCM) team. Access to areas within the datacenter is granted based on the least privilege principle. Before a person arrives at a datacenter, they must have a DCAT request approved by the DCM team. The DCM team reviews the request for a valid business justification and for appropriate access levels. Upon arriving at the datacenter, the individual on the request must have their identification verified by the Control Room Supervisor against a Microsoft identification smart card or a valid government issued identification card or document.  Azure datacenters (leased and fully-managed) utilize physical access devices such as metal detectors, perimeter gates, electronic access smart card readers, biometric readers, man-traps/portals, anti-tailgate devices (in leased datacenters), and anti-pass back controls, as well as security officers to control access to datacenters. As an additional security measure for leased datacenters, Azure has required that anti-tailgating alarms be deployed at the doors to Microsoft colocation rooms.  **Azure Third-Party (Leased) Datacenters**  The physical security requirements of a leased datacenter are designed to reflect similar security capabilities of a fully-managed Azure datacenter. As an additional security measure for leased datacenters, Azure has required that anti-tailgating alarms be deployed at the doors to Microsoft colocation rooms. |
| **Part A2**  **Azure**  Azure enforces physical access authorizations for all physical access points to Azure datacenters. The exteriors of the datacenter buildings are non-descript and do not advertise that they are Microsoft datacenters.  Depending on the design of a datacenter, physical access authorizations at Azure datacenters may begin at a controlled perimeter gate or secured facility door that requires either access smart card authorization or security officer authorization.  Main access to Azure datacenter facilities is restricted to a single point of entry that is manned twenty-four (24) hours a day, seven (7) days a week by security personnel. Emergency exits are alarmed and under video surveillance. Electronic access control devices are installed on doors separating the reception area from the facilities’ interior to restrict access to approved personnel only. Azure datacenters have a security operations desk located in the reception area and in line of sight of the single entry point. The datacenter lobbies have man-trap portal devices that require multifactor authentication such as access card and biometric hand geometry or fingerprint authentication to pass beyond the lobby. Areas within Microsoft datacenters that contain critical systems (e.g., colocations, critical environments, Main Distribution Frame (MDF) rooms, etc.) are further restricted through various security mechanisms such as electronic access control, biometric devices, and anti-passback controls. Additionally, doors are alarmed and under video surveillance.  Access authorizations at Azure datacenters are managed through the Datacenter Access Tool (DCAT). DCAT contains the authorized access lists of personnel who have been approved by the Datacenter Management (DCM) team. Access to areas within the datacenter is granted based on the least privilege principle. Before a person arrives at a datacenter, they must have a DCAT request approved by the DCM team. The DCM team reviews the request for a valid business justification and for appropriate access levels. Upon arriving at the datacenter, the individual on the request must have their identification verified by the Control Room Supervisor against a Microsoft identification smart card or a valid government issued identification card or document.  Azure datacenters (leased and fully-managed) utilize physical access devices such as metal detectors, perimeter gates, electronic access smart card readers, biometric readers, man-traps/portals, anti-tailgate devices (in leased datacenters), and anti-pass back controls, as well as security officers to control access to datacenters. As an additional security measure for leased datacenters, Azure has required that anti-tailgating alarms be deployed at the doors to Microsoft colocation rooms.  **Azure Third-Party (Leased) Datacenters**  The physical security requirements of a leased datacenter are designed to reflect similar security capabilities of a fully-managed Azure datacenter. As an additional security measure for leased datacenters, Azure has required that anti-tailgating alarms be deployed at the doors to Microsoft colocation rooms. |
| **Part B**  **Azure**  Access authorizations at Azure datacenters are managed through the Datacenter Access Tool (DCAT). DCAT contains the authorized access lists of personnel who have been approved by the DCM team. Access to areas within the datacenter is granted based on the least privilege principle. Before a person can be granted physical access to a datacenter, they must have a DCAT request approved by the DCM team. The DCM team reviews the request for a valid business justification and for appropriate access levels. Upon arriving at the datacenter, the individual on the request must have their identification verified by the security against a Microsoft identification smart card or a valid government issued identification card. All accesses to Azure datacenter facilities are logged and audited. |
| **Part C**  **Azure**  Azure datacenters (leased and fully-managed) utilize physical access devices such as metal detectors, perimeter gates, electronic access smart card readers, biometric readers, man-traps/portals, anti-tailgate devices (at leased datacenter locations), and anti-pass back controls, as well as security officers to control access to datacenters. Azure datacenters do not contain areas that are designated as publicly accessible. |
| **Part D**  **Azure**  All visitors that have approved access to the datacenter are designated as “Escort Only” on their badges and are always required to remain with their escorts. Escorted visitors do not have any access levels granted to them and can only travel on the access of their escorts. Escorts monitor all activities of their visitor while in the datacenter. |
| **Part E**  **Azure**  Physical keys and temporary access badges are secured within the datacenter security operations center. Temporary access badges are stored within the access-controlled datacenter security operations center (SOC) and inventoried at the beginning and end of each shift. Security officers are staffed twenty-four (24) hours a day, seven (7) days a week. Physical keys are stored in an electronic key management system. These key management systems are linked to the physical access system and require a security officer’s pin and access smart card to gain access. Keys are checked out to specific personnel by matching the person’s access smart card to the physical key. A person must have the appropriate access level in DCAT to allow them to check out specific keys. Key inventories are conducted during each shift and keys are not allowed to be taken offsite. |
| **Part F**  **Azure**  Physical access devices within Azure datacenters are inventoried on at least an annual basis. Keys and temporary access badges are inventoried multiple times a day at the beginning of each shift. Access smart card readers and similar access devices are linked to the physical security system where status is continuously represented. |
| **Part G**  **Azure**  Azure datacenters have procedures to implement in cases when an access smart card or key is lost or a person is terminated or transferred. In the event of a termination or transfer, the person’s access is immediately removed from the DCAT system and their access smart card removed. This removes any datacenter access the person may have had. DCM teams also perform quarterly access reviews to validate the appropriateness of the datacenter access list in DCAT.  Azure does not require the annual re-keying of locks because Azure datacenters do not use physical keys as a primary access method to the facility. Microsoft’s policy is that no physical keys may leave the site, and no physical keys are permanently issued into individuals. The primary access methods at Azure datacenters are electronic access smart cards and biometrics, which allows for immediate revocation of access as required. Azure mitigates the control risks meant to be addressed by requiring annual re-keying through the primary implementation of electronic and biometric access controls, strict assignment of access levels and controlled distribution and management of keys. Additional security controls such as security patrols, video surveillance, and door alarms help mitigate this risk. Use of keys to open doors in lieu of access smart cards and/or biometrics where required within the datacenters results in a door alarm that requires the Control Room Supervisor to acknowledge the alarm and dispatch a security responder to investigate.  If after an investigation a key was determined to be lost, Azure has procedures in place to determine appropriate action commensurate with the risk that the loss of that specific key has. These actions could require the re-keying of a single server rack or door and up to the re-keying of the entire datacenter facility. |

### PE-3(1) - System Access

Enforce physical access authorizations to the system in addition to the physical access controls for the facility at [physical spaces containing one or more components of the system are defined;].

|  |
| --- |
| **PE-3(1) Control Summary Information** |
| Responsible Roles: Datacenter Hosting |
| Parameter pe-03.01\_odp: areas within Microsoft datacenters that contain critical systems (e.g., colocations, critical environments, Main Distribution Frame (MDF) rooms, etc.) |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **PE-3(1) What is the solution and how is it implemented?** |
| **Azure**  Access authorizations at Azure colocations are managed through the Datacenter Access Tool (DCAT). DCAT contains the authorized access lists of personnel who have been approved by the Datacenter Management (DCM) team. |

## PE-4 Access Control for Transmission

Control physical access to [system distribution and transmission lines requiring physical access controls are defined;] within organizational facilities using [security controls to be implemented to control physical access to system distribution and transmission lines within the organizational facility are defined;].

|  |
| --- |
| **PE-4 Control Summary Information** |
| Responsible Roles: Datacenter Hosting |
| Parameter pe-04\_odp.01: all distribution and transmission lines |
| Parameter pe-04\_odp.02: using badge and biometric authentication |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **PE-4 What is the solution and how is it implemented?** |
| **Azure**  Azure has implemented access control for transmission medium through the design and building of the Main Distribution Frame (MDF) rooms,  Intermediate Distribution Frame (IDF) rooms, and colocations to protect information system distribution and transmission lines from accidental damage, disruption, and physical tampering. Access to MDF rooms, IDF rooms, and colocations require multifactor authentication via access smart card and biometrics. This ensures that access is restricted to only authorized personnel. Within the MDF and IDF, transmission and distribution lines are protected from accidental damage, disruption, and physical tampering using metal conduits, locked racks, cages, or cable trays.  MDF and IDFs where networking equipment for Azure are housed are restricted access areas limited to cleared personnel who have passed an enhanced background screening or by individuals who are escorted while in the MDF and IDF by a person who is cleared and is an authorized government data escort. Signage on these MDF and IDF doors identifies the area as restricted access. |

## PE-5 Access Control for Output Devices

Control physical access to output from [output devices that require physical access control to output are defined;] to prevent unauthorized individuals from obtaining the output.

|  |
| --- |
| **PE-5 Control Summary Information** |
| Responsible Roles: Datacenter Hosting |
| Parameter pe-5: output devices |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **PE-5 What is the solution and how is it implemented?** |
| **Azure**  Azure datacenters do not have output devices (monitors, printers, audio devices, etc.) permanently connected to Azure assets or Azure shared assets. In addition to not having output devices, security officers perform physical walkthroughs of the facility multiple times per shift checking for items like doors being locked and racks being secured. Datacenter access is limited to people who have approved access authorizations. Colocations require multifactor authentication (access smart card and biometrics) to gain access. |

## PE-6 Monitoring Physical Access

a. Monitor physical access to the facility where the system resides to detect and respond to physical security incidents;

b. Review physical access logs [at least monthly] and upon occurrence of [events or potential indication of events requiring physical access logs to be reviewed are defined;] ; and

c. Coordinate results of reviews and investigations with the organizational incident response capability.

|  |
| --- |
| **PE-6 Control Summary Information** |
| Responsible Roles: Datacenter Hosting |
| Parameter pe-06\_odp.01: continuously |
| Parameter pe-06\_odp.02: indications or a report of an incident |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **PE-6 What is the solution and how is it implemented?** |
| **Part A**  **Azure**  Physical access is monitored by implementing security devices and processes at the datacenters. Examples include twenty-four (24) hours a day, seven (7) days a week electronic monitoring of access control, alarm and video systems as well as twenty-four (24) hours a day, seven (7) days a week on site security patrols of the facility and grounds. A Control Room Supervisor is located in the datacenter security operations center at all times to provide monitoring of physical access in the datacenter.  CCTV is employed to monitor physical access to the datacenter and the information system. The CCTV is linked to the building alarm monitoring system to provide physical access monitoring of alarm points. Cameras are positioned to monitor perimeter doors, facility entrances and exits, all colocation rows and aisles, all racks, caged areas, high-security areas, shipping and receiving, facility external areas such as parking lots and other areas of the facility.  Security officers provide Azure with a security program staffed with highly-trained security officers capable of accomplishing the following:  \* Ensuring that only those personnel with proper authorization are allowed access to Azure Critical Infrastructure.  \* Ensuring that personnel and visitors bringing equipment into and out of critical infrastructure facilities follow proper procedures to prevent intentional or unintentional loss.  \* Constant patrolling allows officers to respond to, observe and report all incidents that may compromise the security at Microsoft. All incidents observed are reported to the Control Room Supervisor.  \* Identify, escalate, and prevent criminal or unsafe activity, and be familiar with, adhere to, and enforce Azure policies and procedures. |
| **Part B**  **Azure**  To access an Azure datacenter, a person must have a DCAT request approved by the Datacenter Management (DCM) team. In order to enter an Azure datacenter, a person must check-in with the datacenter security operations center (SOC) to facilitate/activate their access that is manned twenty-four (24) hours a day, seven (7) days a week. A person’s physical access within the datacenter is reviewed continuously by the Control Room Supervisor in the SOC. The Control Room Supervisor monitors live camera feeds within the datacenter as well as the alarm monitoring system reports from all physical security access devices within the datacenter. Physical access is reported in the alarm monitoring system as approved or failed. Failed access results in an alarm status that requires action by the Control Room Supervisor. The Control Room Supervisor can dispatch a responder for further investigation if needed. The physical access logs in the alarm monitoring system are reviewed continuously but are also available log files for subsequent investigative review. |
| **Part C**  **Azure**  Security events that occur within the datacenter are documented by the security team in a report called a Significant Event Notification (SEN). SEN reports capture the details of a security event and are required to be documented after an event occurs in order to capture details as accurately as possible.  SEN reports also contain the investigative analysis conducted in an After Action Report (AAR). AAR reports document the investigation into a security event and attempts to identify the root cause of the event. Additionally, any remediation actions or lessons learned are also included in the AAR, so that security procedures can be improved across the Azure datacenter security program. In the event an incident impacts Azure assets or services, the Azure Security Response Team has procedures in place to respond to and report such incidents. For incidents requiring government notification, the Security Response Team coordinates with the service team to notify the government agency customer, US-CERT, and authorizing officials within US-CERT guidelines.  **Azure Third-Party (Leased) Datacenters**  At leased datacenter locations, security events are communicated to the DCM team and escalated based on severity. The DCM team determines additional investigation or escalation. |

### PE-6(1) - Intrusion Alarms and Surveillance Equipment

Monitor physical access to the facility where the system resides using physical intrusion alarms and surveillance equipment.

|  |
| --- |
| **PE-6(1) Control Summary Information** |
| Responsible Roles: Datacenter Hosting |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **PE-6(1) What is the solution and how is it implemented?** |
| **Azure**  In addition to the twenty-four (24) hours a day, seven (7) days a week onsite security, Azure datacenters also utilize alarm monitoring systems. This provides real-time alarm and video monitoring. Datacenter doors have alarms that report when being opened or when they remain open passed a programmed length of time. Doors can also be programmed to display the live CCTV image when a door alarm is triggered. Additionally, the Control Room Supervisor constantly monitors a live feed of camera views from high security and high traffic areas. DCAT is also used to control access smart card management (creation and modification). Access card and biometric hand geometry and fingerprint readers are programmed and monitored through the alarm monitoring system. Alarms are monitored and responded to by the Control Room Supervisor stationed twenty-four (24) hours a day, seven (7) days a week in the datacenter security operations center. During a response situation, the Control Room Supervisor utilizes cameras in the area of the incident being investigated to give the responder real-time information. |

### PE-6(4) - Monitoring Physical Access to Systems

Monitor physical access to the system in addition to the physical access monitoring of the facility at [physical spaces containing one or more components of the system are defined;].

|  |
| --- |
| **PE-6(4) Control Summary Information** |
| Responsible Roles: Datacenter Hosting |
| Parameter pe-06.04\_odp: perimeter doors, facility entrances and exits, interior aisles, caged areas, high-security areas, shipping and receiving, facility external areas such as parking lots and other areas of the facility |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **PE-6(4) What is the solution and how is it implemented?** |
| **Azure**  In addition to the physical access monitoring of the facility, Azure monitors the physical access to the assets within the datacenters. All Microsoft’s online services’ equipment is placed in locations within datacenters where physical access is monitored. All colocation and Main Distribution Frame (MDF) rooms are protected by access control, alarms, and video. |

## PE-8 Visitor Access Records

a. Maintain visitor access records to the facility where the system resides for [for a minimum of one (1) year];

b. Review visitor access records [at least monthly] ; and

c. Report anomalies in visitor access records to [personnel to whom visitor access records anomalies are reported to is/are defined;].

|  |
| --- |
| **PE-8 Control Summary Information** |
| Responsible Roles: Datacenter Hosting |
| Parameter pe-08\_odp.01: for a minimum of one (1) year |
| Parameter pe-08\_odp.02: at least monthly |
| Parameter pe-08\_odp.03: MSRC |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **PE-8 What is the solution and how is it implemented?** |
| **Part A**  **Azure**  Visitor datacenter access records are maintained in DCAT in the form of approved DCAT requests . DCAT requests can only be approved by the Datacenter Management (DCM) team. All visitor access requests to Azure datacenters is recorded in DCAT and is available for future possible investigations. Visitors are always required to be escorted and are not granted any access to Azure datacenters. The escort’s access within the datacenter is logged within Lenel OnGuard Alarm Monitoring System and, if necessary, can be correlated to the visitor for future review.  **Azure Third-Party (Leased) Datacenters**  For leased datacenters, Azure is provided monthly with a log of all access attempts to the Microsoft areas.  Visitor access records processed for both owned and leased Azure datacenters are retained for 3 years. |
| **Part B**  **Azure**  Visitors are always required to be escorted. The escort’s access within the datacenter is logged within the alarm monitoring system and if necessary can be correlated to the visitor for future review . Visitor access is being reviewed continuously by the assigned escort and by the control room supervisor via CCTV and the alarm monitoring system. Visitors are not provided with access and must always be accompanied by their escorts.  Visitors with an approved DCAT access request have their access request reviewed at the time their identification is verified against a form of a valid government issued ID or Microsoft issued smart card. Visitors are always escorted while at the datacenter. Visitors approved for escorted access are issued a sticky badge. Additionally, when a visitor concludes their visit by returning their sticky badge to the CRS, the CRS terminates the visitor’s DCAT access record during a final review. Azure maintains visitor access records within the DCAT database for possible future investigations. Additionally, visitors assigned a Visitor or Tour access level in DCAT are always required to have an escort present. The escort is responsible for reviewing the actions and access of their visitor during their visit to the datacenter.  **Azure Third-Party (Leased) Datacenters**  At leased datacenter locations, visitors to Microsoft areas are always required to be escorted and wear a badge that indicates their visitor status. The escort is responsible for reviewing the actions and access of their visitor during their visit to the datacenter. |
| **Part C**  **Azure**  Visitor datacenter access records are maintained in DCAT in the form of approved DCAT requests . DCAT requests can only be approved by the Datacenter Management (DCM) team. All visitor access requests to Azure datacenters is recorded in DCAT and is available for future possible investigations. Visitors are always required to be escorted and are not granted any access to Azure datacenters. The escort’s access within the datacenter is logged within Lenel OnGuard Alarm Monitoring System and, if necessary, can be correlated to the visitor for future review. Anomalies in visitor access records are reported to Datacenter Management and Security Teams for investigation.  **Azure Third-Party (Leased) Datacenters**  For leased datacenters, Azure is provided monthly with a log of all access attempts to the Microsoft areas.  Visitor access records processed for both owned and leased Azure datacenters are retained for 3 years. Anomalies in visitor access records are reported to Datacenter Management and Security Teams for investigation. |

### PE-8(1) - Automated Records Maintenance and Review

Maintain and review visitor access records using [Assignment: organization-defined automated mechanisms].

|  |
| --- |
| **PE-8(1) Control Summary Information** |
| Responsible Roles: Datacenter Hosting |
| Parameter pe-8.1\_prm\_1: the Datacenter Access Tool (DCAT) |
| Parameter pe-08.01\_odp.01: |
| Parameter pe-08.01\_odp.02: |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **PE-8(1) What is the solution and how is it implemented?** |
| **Azure**  Datacenter access records are maintained in DCAT in the form of approved DCAT requests. DCAT requests can only be approved by the Datacenter Management (DCM) team. Access levels within the datacenter are assigned and managed within DCAT. Datacenter access is reviewed quarterly. All access to Azure datacenters is recorded in DCAT and is available for future possible investigations. Visitors are always required to be escorted. The escort’s access within the datacenter is logged within the alarm monitoring system and if necessary can be correlated to the visitor for future review. Visitor access is being reviewed continuously by the assigned escort and by the control room supervisor via CCTV and the alarm monitoring system. Visitors are not provided with access and must always be accompanied by their escorts.  Datacenter access records are maintained in DCAT in the form of approved DCAT requests. DCAT is the automated mechanism used to maintain and review visitor access records. DCAT requests can only be approved by the DCM team. Access levels within the datacenter are assigned and managed within DCAT. Datacenter access is reviewed quarterly. All access to Azure datacenters is recorded in DCAT and is available for future possible investigations . Visitors are always required to be escorted. The escort’s access within the datacenter is logged within the alarm monitoring system and if necessary can be correlated to the visitor for future review. Visitor access is being reviewed continuously by the assigned escort and by the control room supervisor via CCTV and the alarm monitoring system. Visitors are not provided with access and must always be accompanied by their escorts. |

## PE-9 Power Equipment and Cabling

Protect power equipment and power cabling for the system from damage and destruction.

|  |
| --- |
| **PE-9 Control Summary Information** |
| Responsible Roles: Datacenter Hosting |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **PE-9 What is the solution and how is it implemented?** |
| **Azure**  Azure provides protective spaces and appropriate labeling for cables. Azure equipment such as cables, electrical lines, and backup generators must be placed in environments which have been engineered to be protected from environmental risks such as theft, fire, explosives, smoke, water, dust, vibration, earthquake, harmful chemicals, electrical interference, power outages, electrical disturbances (spikes). All portable online services’ assets (e.g. racks, servers, network devices) must be locked or fastened in place to provide protection against theft or movement damage. Power and information system cables within any Azure environment are labeled appropriately and protected against interception or damage. Power and information system cables are separated from each other at all points within an environment to avoid interference. Power cables are run under the floors, overhead in cable trays and within cabinets for protection from moving parts and accidental damage. All electrical spaces are behind card readers or additional key locks as appropriate. Access hallways as well as exterior entrances and equipment yards approaching the protective spaces are all monitored via video surveillance.  Power systems also utilize redundancy as a form of protection. Datacenters utilize multiple power/utility feeds into the facility as well as redundant configurations of generators and UPS systems. Generator and UPS system components undergo regular maintenance procedures to maintain the systems in proper working order. |

## PE-10 Emergency Shutoff

a. Provide the capability of shutting off power to [system or individual system components that require the capability to shut off power in emergency situations is/are defined;] in emergency situations;

b. Place emergency shutoff switches or devices in [near more than one egress point of the IT area and ensures it is labeled and protected by a cover to prevent accidental shut-off] to facilitate access for authorized personnel; and

c. Protect emergency power shutoff capability from unauthorized activation.

|  |
| --- |
| **PE-10 Control Summary Information** |
| Responsible Roles: Datacenter Hosting |
| Parameter pe-10\_odp.01: equipment in colocations or staffed Facilities Operation Centers (FOCs) |
| Parameter pe-10\_odp.02: near more than one egress point of the IT area and ensures it is labeled and protected by a cover to prevent accidental shut-off |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **PE-10 What is the solution and how is it implemented?** |
| **Part A**  **Azure**  Azure has installed Emergency Power Off (EPO) Buttons in locations within the datacenter only as required by local fire code.  **Azure Third-Party (Leased) Datacenters**  Azure leased datacenters may have EPO buttons installed at the colocation rooms at the discretion of the colocation provider, but this is not currently required by Microsoft. |
| **Part B**  **Azure**  When present, EPO buttons are strategically placed to allow for activation in emergency situations. EPO buttons can be placed in the colocations, manned Facilities Operation Centers (FOCs), or as required by local fire code. In most Azure datacenters, the datacenter design no longer requires EPO buttons. |
| **Part C**  **Azure**  When present, to prevent accidental activation, EPO buttons may have a protective enclosure, require dual activation, or utilize an audible alarm as a warning before activation. Additionally, EPO buttons are under video surveillance. |

## PE-11 Emergency Power

Provide an uninterruptible power supply to facilitate [Selection: an orderly shutdown of the system;transition of the system to long-term alternate power] in the event of a primary power source loss.

|  |
| --- |
| **PE-11 Control Summary Information** |
| Responsible Roles: Datacenter Hosting |
| Parameter pe-11: transition of the information system to long-term alternate power |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **PE-11 What is the solution and how is it implemented?** |
| **Azure**  Azure has implemented emergency power by protecting datacenter equipment and circuits with an Uninterruptable Power Supply (UPS) system which provides a short-term power supply to provide power until generators are able to come online. Azure utilizes various forms of UPS systems and generators throughout its datacenters.  Azure has implemented the control for emergency power by protecting datacenter equipment and circuits with an uninterruptible power supply (UPS) system which provides a short-term power supply until generators are able to come online and transition the load. Azure utilizes various forms of UPS systems and generators throughout its datacenters. Azure datacenters are designed with at least an n+1 configuration for electrical and cooling systems. Azure datacenters maintain sufficient onsite fuel storage to operate for approximately 48 hours. Alternate refueling agreements are required in order to ensure a fuel supply is available in the event of a long term utility power loss.  **Azure Third-Party (Leased) Datacenters**  Azure requires that its leased datacenter providers be capable of providing sufficient UPS power to allow for the transition of the system's full load to generator power. Azure also requires that onsite power generation be capable of sustaining the system's full load for 48 hours with on-site fuel stores. Azure requires that its leased datacenter providers also have alternate fuel agreements in place to allow for refueling. |

### PE-11(1) - Alternate Power Supply - Minimal Operational Capability

Provide an alternate power supply for the system that is activated [Selection: manually;automatically] and that can maintain minimally required operational capability in the event of an extended loss of the primary power source.

|  |
| --- |
| **PE-11(1) Control Summary Information** |
| Responsible Roles: Datacenter Hosting |
| Parameter pe-11.01\_odp: automatically |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **PE-11(1) What is the solution and how is it implemented?** |
| **Azure**  In the event of an extended loss of the primary power source, Azure implements a long-term alternate power supply for the information system that can maintain minimally required operational capability. When power fails or drops to an unacceptable voltage level, Uninterruptable Power Supply (UPS) systems instantly kick in and take over the power load. This provides enough power for running the servers until the generators can take over. Emergency generators provide back-up power for extended outages and for planned maintenance and can operate the datacenter with on-site fuel reserves in the event of a natural disaster. Azure maintains diesel generator at many of its datacenters. Backup generators are used when necessary to help maintain grid stability or in extraordinary repair, and maintenance situations that require us to take our datacenters off the power grid.  Azure datacenters are designed with at least an n+1 configuration for electrical and cooling systems. Azure datacenters maintain sufficient onsite fuel storage to operate for approximately 48 hours. Alternate refueling agreements are required in order to ensure a fuel supply is available in the event of a long term utility power loss. |

## PE-12 Emergency Lighting

Employ and maintain automatic emergency lighting for the system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

|  |
| --- |
| **PE-12 Control Summary Information** |
| Responsible Roles: Datacenter Hosting |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **PE-12 What is the solution and how is it implemented?** |
| **Azure**  Azure datacenters implement emergency lighting in the form of overhead emergency lighting on dedicated circuits backed up by UPS and generator systems. Automatic emergency lighting is implemented along all evacuation routes, emergency exits, and inside the colocations in accordance with the National Fire and Protection Association (NFPA) Life Safety Code. If utility power is lost, the emergency lighting automatically switches to power provided by the UPS and generator systems. The emergency lighting systems within Azure datacenters undergo routine maintenance to ensure that they remain in proper working order. |

## PE-13 Fire Protection

Employ and maintain fire detection and suppression systems that are supported by an independent energy source.

|  |
| --- |
| **PE-13 Control Summary Information** |
| Responsible Roles: Datacenter Hosting |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **PE-13 What is the solution and how is it implemented?** |
| **Azure**  Azure has implemented fire protection by installing fire detection and fire suppression systems at the Azure datacenters. Azure datacenters implement robust fire detection mechanisms. The Azure fire protection approach includes the use of photoelectric smoke detectors installed below the floor and on the ceiling, which are integrated with the fire protection sprinkler system. Additionally, there are Very Early Smoke Detection Apparatus (VESDA) systems in each colocation which monitor the air. VESDA units are highly sensitive air sampling systems installed throughout multiple high-value spaces. VESDA units allow for an investigative response prior to an actual fire detection alarm.  Pull station fire alarm boxes are installed throughout the datacenters for manual fire alarm notification. Fire extinguishers are located throughout the datacenters and are properly inspected, serviced, and tagged annually. The security staff patrols all building areas multiple times every eight (8) hour shift. The Critical Environments (CE) Team does a daily site walk-through checking on each non-monitored room and many component parts in each non-monitored room ensuring all fire watch requirements are being met.  Areas containing sensitive electrical equipment (colocations, Main Distribution Frames (MDFs), etc.) are protected by double interlock pre-action (dry pipe) sprinkler systems. Dry pipe sprinklers are a two-stage pre-action system that requires both a sprinkler head activation (due to heat) as well as smoke detection to release water. The sprinkler head activation releases the air pressure in the pipes which allows the pipes to fill with water. Water is released when a smoke or heat detector is also activated.  Fire detection/suppression and emergency lighting systems are wired into the datacenter UPS and generator systems providing for a redundant power source. |

### PE-13(1) - Detection Systems - Automatic Activation and Notification

Employ fire detection systems that activate automatically and notify [service provider building maintenance/physical security personnel] and [service provider emergency responders with incident response responsibilities] in the event of a fire.

|  |
| --- |
| **PE-13(1) Control Summary Information** |
| Responsible Roles: Datacenter Hosting |
| Parameter pe-13.01\_odp.01: local security staff |
| Parameter pe-13.01\_odp.02: local fire department |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **PE-13(1) What is the solution and how is it implemented?** |
| **Azure**  Azure employs fire detection devices/systems for the information system that activate automatically and notify datacenter personnel along with emergency responders in the event of a fire.  Fire detection includes photoelectric smoke detectors installed below the floor and on the ceiling and smoke detection systems such as the Xtralis Very Early Smoke Detection Apparatus (VESDA) systems, as well as pull station fire alarms for manual fire alarm notification.  If one of the fire detection mechanisms is activated in any colocation, the local fire department is automatically notified through a contracted third-party monitoring vendor. In addition, the fire protection and fire detection systems are tied into the security system notifying the local facility and security staff . |

### PE-13(2) - Suppression Systems - Automatic Activation and Notification

(a) Employ fire suppression systems that activate automatically and notify [personnel or roles to be notified in the event of a fire is/are defined;] and [emergency responders to be notified in the event of a fire are defined;] ; and

(b) Employ an automatic fire suppression capability when the facility is not staffed on a continuous basis.

|  |
| --- |
| **PE-13(2) Control Summary Information** |
| Responsible Roles: Datacenter Hosting |
| Parameter pe-13.02\_odp.01: local security staff |
| Parameter pe-13.02\_odp.02: local fire department |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **PE-13(2) What is the solution and how is it implemented?** |
| **Part A**  **Azure**  If one of the fire suppression systems is activated at the datacenter, the local fire department is automatically notified through the fire alarm system . In addition, the fire protection and fire detection systems are tied into the security system notifying the local facility and security staff.Azure datacenters are staffed twenty-four (24) hours a day, seven (7) days a week. Fire suppression systems engage automatically without manual intervention when a fire alarm situation is detected. |
| **Part B**  **Azure**  If one of the fire suppression systems is activated at the datacenter, the local fire department is automatically notified through the fire alarm system . In addition, the fire protection and fire detection systems are tied into the security system notifying the local facility and security staff.Azure datacenters are staffed twenty-four (24) hours a day, seven (7) days a week. Fire suppression systems engage automatically without manual intervention when a fire alarm situation is detected. Automatic fire suppression capability is deployed in addition staffing. |

## PE-14 Environmental Controls

a. Maintain [Selection (OneOrMore): temperature;humidity;pressure;radiation;[environmental control(s) for which to maintain a specified level in the facility where the system resides are defined (if selected);] ] levels within the facility where the system resides at [acceptable levels for environmental controls are defined;] ; and

b. Monitor environmental control levels [continuously].

(a) Requirement: The service provider measures temperature at server inlets and humidity levels by dew point.

|  |
| --- |
| **PE-14 Control Summary Information** |
| Responsible Roles: Datacenter Hosting |
| Parameter pe-14\_odp.01: temperature, humidity, and pressure consistent with American Society of Heating, Refrigerating and Air-conditioning Engineers (ASHRAE) document entitled Thermal Guidelines for Data Processing Environments |
| Parameter pe-14\_odp.02: |
| Parameter pe-14\_odp.03: levels in accordance with Microsoft datacenter guidelines |
| Parameter pe-14\_odp.04: continuously |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **PE-14 What is the solution and how is it implemented?** |
| **Part A**  **Azure**  Azure maintains the temperature and humidity levels in accordance with Microsoft datacenter guidelines. The temperature and humidity levels are monitored continuously by the datacenter’s Building Management System (BMS). |
| **Part B**  **Azure**  At Azure datacenters, temperature and humidity levels are monitored continuously by the Building Management System (BMS). CE team members monitor the BMS from the Facilities Operations Center (FOC), so that they can manage the temperature and humidity within the datacenter before any alarm points are exceeded. BMS is configured with several notification points.  As the temperature or humidity approaches these points, notifications are sent so that the CE team can be dispatched for investigation or able to make adjustments to remediate the temperature or humidity within the datacenter. The acceptable datacenter temperature range within cold aisles is between 65 degrees and 95 degrees Fahrenheit. In certain instances, the temperature may require adjustment outside of this range to address local geographical and meteorological factors.  Datacenter humidity is measured by Relative Humidity percentage, Non-Condensing with the current acceptable range between 10% and 80%. |

### PE-14(2) - Monitoring with Alarms and Notifications

Employ environmental control monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment to [personnel or roles to be notified by environmental control monitoring when environmental changes are potentially harmful to personnel or equipment is/are defined;].

|  |
| --- |
| **PE-14(2) Control Summary Information** |
| Responsible Roles: Datacenter Hosting |
| Parameter pe-14.02\_odp: CE team members |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **PE-14(2) What is the solution and how is it implemented?** |
| **Azure**  At Azure datacenters, temperature and humidity levels are monitored continuously by the Building Management System (BMS). CE team members monitor the BMS from the Facilities Operations Center (FOC), so that they can manage the temperature and humidity within the datacenter before any alarm points are exceeded. BMS is configured with several notification points. As the temperature or humidity approaches these points, notifications are sent so that the CE team can be dispatched for investigation or able to adjust the temperature or humidity within the datacenter. |

## PE-15 Water Damage Protection

Protect the system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

|  |
| --- |
| **PE-15 Control Summary Information** |
| Responsible Roles: Datacenter Hosting |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **PE-15 What is the solution and how is it implemented?** |
| **Azure**  Azure provides water and leak detection in areas with a risk of water leakage, such as near Air Handlers Units. Fire suppression systems also have leak detection alarms that are monitored. The water/leak detection system is integrated with the facility alarm and notification system. The sprinkler systems in the datacenters are zoned. The Critical Environment (CE) team and Datacenter Management (DCM) teams are familiar with emergency procedures requiring the use of the water shutoff valves and their locations. The sprinkler risers can be shut off individually or as a group via gate valves. All sprinklers in the critical space are double interlock pre-action type sprinklers that require two forms of activation before flow is initiated. The pressure of the sprinkler system is monitored and alarmed against water leakage. |

### PE-15(1) - Automation Support

Detect the presence of water near the system and alert [service provider building maintenance/physical security personnel] using [automated mechanisms used to detect the presence of water near the system are defined;].

|  |
| --- |
| **PE-15(1) Control Summary Information** |
| Responsible Roles: Datacenter Hosting |
| Parameter pe-15.01\_odp.01: local security staff |
| Parameter pe-15.01\_odp.02: automated leak detection mechanisms |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **PE-15(1) What is the solution and how is it implemented?** |
| **Azure**  Azure employs automated mechanism to detect water presence in the datacenters and alerts datacenter personnel. Azure provides water/leak detection in areas with a risk of water leakage (e.g. Air Handlers Units). Fire suppression systems also have leak detection alarms that are monitored. The water/leak detection system is integrated with the facility alarm and notification system. The pressure of the sprinkler system is monitored and alarmed against water leakage. |

## PE-16 Delivery and Removal

a. Authorize and control [all information system components] entering and exiting the facility; and

b. Maintain records of the system components.

|  |
| --- |
| **PE-16 Control Summary Information** |
| Responsible Roles: Datacenter Hosting |
| Parameter pe-16(a): all information system components |
| Parameter pe-16\_odp.01: |
| Parameter pe-16\_odp.02: |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **PE-16 What is the solution and how is it implemented?** |
| **Azure**  Assets that are to be destroyed are stored in locked storage bins that are under CCTV camera coverage. When the assets are ready to be destroyed, the locked storage bins are moved to shredding locations by Microsoft full time employee (FTE) from Asset Management. As shredding occurs at the datacenter and under Microsoft supervision, Azure assets do not leave the controlled areas of the datacenter.  Azure implements strict enforcement of what is allowed to enter and exit the datacenter. All system components/assets are tracked in the asset management tool database.  Information system component deliveries must be scheduled; unscheduled deliveries are refused entry past the datacenter gates. Deliveries are received in the facilities loading bay. The facilities asset manager must be present during the delivery. The loading bay is monitored with a live CCTV feed in the datacenter security operations center. In datacenters where the loading bay is adjacent to the staging area, the loading bay doors are designed in an interlock configuration, so that if the loading bay door is open for a delivery truck, the interior door to the staging area is not capable of being opened.  When an information system component enters the building, the asset management team verifies the received item against the referenced ticket and then scans the device into Azure-managed asset management tool. New assets are unpacked in the staging area and stored in the asset management room until deployment. Depending on asset value, some high value assets are stored in separate locked cages with cameras. The general storage area within the asset management room requires an access smart card for entry and has multiple cameras for video monitoring.  For an information system component that is leaving the datacenter, a ticket request must be generated on the system owner’s behalf via the asset deployment tool. All data is removed from the system (i.e. hard drives wiped or purged depending on asset classification) before leaving the datacenter. All information system components received or shipped are tracked by the workflow ticketing tool and/or in the receiving/shipping logs in the asset management tool.  Visitors are prohibited from using personal laptops or cell phones with camera capabilities in the production environment (colocations) per the datacenter policy and work rules. If the equipment entering the datacenter is used for maintenance purposes, the equipment requires datacenter management approval in the DCAT system.  **Azure Third Party (Leased) Datacenters**  In leased datacenters, the loading bay area is controlled by the datacenter provider. To manage entry and exit of Azure system components, an Azure representative must be present during the process. |

## PE-17 Alternate Work Site

a. Determine and document the [alternate work sites allowed for use by employees are defined;] allowed for use by employees;

b. Employ the following controls at alternate work sites: [controls to be employed at alternate work sites are defined;];

c. Assess the effectiveness of controls at alternate work sites; and

d. Provide a means for employees to communicate with information security and privacy personnel in case of incidents.

|  |
| --- |
| **PE-17 Control Summary Information** |
| Responsible Roles: Datacenter Hosting |
| Parameter pe-17\_odp.01: alternate work sites |
| Parameter pe-17\_odp.02: appropriate management, operational, and technical controls defined for alternate work sites |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **PE-17 What is the solution and how is it implemented?** |
| **Part A**  **Azure**  Azure identifies designated Microsoft campuses and telecommuting locations as the alternate worksites. Azure has implemented appropriate management, operational and technical controls at these facilities i.e. all Azure datacenters in the US have the same controls implemented as documented in this SSP. These controls are assessed to assure the effectiveness of the security measures. Access control such as access to the alternate work sites are monitored regularly and visitors are required to check in with receptionist. Telecommuting locations are governed by the Microsoft remote access policy which requires remote access to production Microsoft’s online services’ networks to employ authentication mechanisms.  Microsoft owns multiple buildings from which Microsoft personnel can work from in the case of an emergency in a building or set of buildings. Microsoft buildings are built and operated to the same security standards. |
| **Part B**  **Azure**  Azure testing procedures based on NIST Special Publication 800-53A Revision 5 are assessed at each datacenter, regardless if they are designated as primary or alternate sites for applications supported in the environment. Azure implements the same controls at each of these work sites, as each site supports various Microsoft properties. Depending on capacity, each datacenter can be used as an alternate to another and is built to identical physical, environmental, and security standards. The security controls at each datacenter are identical and in accordance with the procedures outlined in the Physical Security Operations Standard Operating Procedure (SOP). All datacenter work is performed by Microsoft personnel who are cleared, trained, and authorized to work within the datacenter environment. |
| **Part C**  **Azure**  In the event of a security incident, datacenter personnel can communicate to each other using handheld radios and cell phones. During an incident one practice is to create a conference bridge to allow for communication with alternate worksites and the Security Response Team. In addition, Azure personnel are trained on incident management capabilities. This training is conducted at least annually. |

## PE-18 Location of System Components

Position system components within the facility to minimize potential damage from [physical and environmental hazards identified during threat assessment] and to minimize the opportunity for unauthorized access.

|  |
| --- |
| **PE-18 Control Summary Information** |
| Responsible Roles: Datacenter Hosting |
| Parameter pe-18: physical and environmental hazards such as theft, fire, explosives, smoke, water, dust, vibration, earthquake, harmful chemicals, electrical interference, power outages, electrical disturbances (spikes), and radiation |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **PE-18 What is the solution and how is it implemented?** |
| **Azure**  Azure implements strategic datacenter design approach to satisfy the location of information system components control. All Microsoft’s online services’ equipment is placed in locations which have been engineered to be protected from environmental risks such as theft, fire, explosives, smoke, water, dust, vibration, earthquake, harmful chemicals, electrical interference, power outages, electrical disturbances (spikes), and radiation. The facility and infrastructure have implemented seismic bracing for protection against environmental hazards. All colocation and Main Distribution Frame (MDF) rooms are protected by access control, alarms, and video. The facility is also patrolled by security officers twenty-four (24) hours a day, seven (7) days a week. All portable Azure assets are locked or fastened in place to provide protection against theft or movement damage. |

# Planning (PL)

## PL-1 Policy and Procedures

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (OneOrMore): organization-level;mission/business process-level;system-level] planning policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the planning policy and the associated planning controls;

b. Designate an [an official to manage the planning policy and procedures is defined;] to manage the development, documentation, and dissemination of the planning policy and procedures; and

c. Review and update the current planning:

1. Policy [at least annually] and following [events that would require the current planning policy to be reviewed and updated are defined;] ; and

2. Procedures [at least annually] and following [significant changes].

|  |
| --- |
| **PL-1 Control Summary Information** |
| Responsible Roles: SOP Team, Policy |
| Parameter pl-1(a): all personnel |
| Parameter pl-01\_odp.01: |
| Parameter pl-01\_odp.02: |
| Parameter pl-01\_odp.03: a Microsoft-wide |
| Parameter pl-01\_odp.04: the Microsoft Information Risk Management Council (IRMC) organization |
| Parameter pl-01\_odp.05: at least annually |
| Parameter pl-01\_odp.06: significant changes |
| Parameter pl-01\_odp.07: at least annually |
| Parameter pl-01\_odp.08: significant changes |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☒ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **PL-1 What is the solution and how is it implemented?** |
| **Part A1**  **Customer Responsibility**  The customer is responsible for developing, documenting, and disseminating planning protection policy and procedures that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.  **Azure**  Azure addresses the planning policy as part of the Microsoft security policies, of which there are two sets: the Microsoft Security Policy (MSP) that is applicable to all personnel, and the Microsoft Security Program Policy (MSPP), which is applicable to all Microsoft personnel that have a responsibility for security. The Microsoft Information Risk Management Council (IRMC) is the governance body with review and approval responsibility for the MSP and MSPP. The MSPP specifically applies to all Microsoft personnel with security objectives such as designing, building, and operating Azure and across all information and processes used in the conduct of Microsoft business. All Azure personnel are accountable and responsible for complying with these guiding principles within their designated roles. The policy addresses the following:  \* Security policy  \* Security roles and responsibilities  Additionally, the policy addresses the purpose, scope, roles, responsibilities, compliance requirements, and required coordination among the various Microsoft organizations that provide some level of support to all services. The standards indicate Microsoft management’s commitment and are a component of the risk management strategy which provides Azure personnel with a current set of clear and concise information security requirements.  The MSP is available to all Microsoft personnel on the Microsoft Policy website on the Microsoft intranet, and the MSPP and Security Standards are available through the Liquid tool, also on the Microsoft intranet. The Azure SOPs are stored in the Azure Security, Privacy & Compliance SharePoint site. This SharePoint site is accessible to all Azure personnel.  Service teams may supplement the Azure policies and procedures with offering-specific policies and procedures. Service-team-specific policies and procedures associated with planning are documented and stored within internal Azure SharePoint sites. Only personnel with authorized credentials, adequate levels of permission, legitimate need to know, and specific roles and responsibilities are given access to the service-team-specific policies or procedures. |
| **Part A2**  **Customer Responsibility**  The customer is responsible for procedures to facilitate the implementation of the planning policy and the associated planning controls.  **Azure**  The Azure Security Assessment and Authorization Standard Operating Procedure (SOP) implements the planning policy and associated controls and documents the following procedures:  \* Documentation  \* Plans of action and milestones  Service teams may supplement the Azure policies and procedures with offering-specific policies and procedures. Service-team-specific policies and procedures associated with planning are documented and stored within internal Azure SharePoint sites. Only personnel with authorized credentials, adequate levels of permission, legitimate need to know, and specific roles and responsibilities are given access to the service-team-specific policies or procedures. |
| **Part B**  **Customer Responsibility**  The customer is responsible for designating an official to manage the development, documentation, and dissemination of the planning policy and procedures.  **Azure**  The Microsoft Information Risk Management Council (IRMC) organization is the governance body with approval responsibility for the Microsoft Security Policy (MSP) and Microsoft Security Program Policy (MSPP). The IRMC consists of representatives from security and risk management teams across Microsoft including Core Services Engineering and Operations (CSEO), Azure, and Global Security. The Customer Security and Trust: Security Engineering (CST-SE) organization manages the review and approval process and maintains the policies.  On an annual basis, the CST-SE conducts a line-by-line review of the MSP and MSPP. The Microsoft Security Policy (MSP) and Microsoft Security Program Policy (MSPP) Governance document describes each member’s role, types and frequency of review, escalation paths, approval process, and formal publishing procedures of the security policy. Throughout the year, if necessary, CST-SE may convene with the IRMC to conduct reviews after a significant review or change request. The approved policy update is published within the relevant tool on the Microsoft intranet. If service teams establish service-specific or team-specific policies, the respective service teams update the necessary policies at least annually. |
| **Part C1**  **Customer Responsibility**  The customer is responsible for reviewing and updating the current planning policy on a regular basis and following organization defined events.  **Azure**  The Azure team updates the Azure SOPs at least annually through a formal review process. If needed, the Azure team updates the SOP after a significant change affecting policy execution as well. If established, service-team-specific procedures are updated by their respective teams. The individual service teams review and update their respective SOPs at least annually and when required by a significant change. |
| **Part C2**  **Customer Responsibility**  The customer is responsible for reviewing and updating the current planning procedures on a regular basis and following organization defined events.  **Azure**  The Azure team updates the Azure SOPs at least annually through a formal review process. If needed, the Azure team updates the SOP after a significant change affecting policy execution as well. If established, service-team-specific procedures are updated by their respective teams. The individual service teams review and update their respective SOPs at least annually and when required by a significant change. |

## PL-2 System Security and Privacy Plans

a. Develop security and privacy plans for the system that:

1. Are consistent with the organization's enterprise architecture;

2. Explicitly define the constituent system components;

3. Describe the operational context of the system in terms of mission and business processes;

4. Identify the individuals that fulfill system roles and responsibilities;

5. Identify the information types processed, stored, and transmitted by the system;

6. Provide the security categorization of the system, including supporting rationale;

7. Describe any specific threats to the system that are of concern to the organization;

8. Provide the results of a privacy risk assessment for systems processing personally identifiable information;

9. Describe the operational environment for the system and any dependencies on or connections to other systems or system components;

10. Provide an overview of the security and privacy requirements for the system;

11. Identify any relevant control baselines or overlays, if applicable;

12. Describe the controls in place or planned for meeting the security and privacy requirements, including a rationale for any tailoring decisions;

13. Include risk determinations for security and privacy architecture and design decisions;

14. Include security- and privacy-related activities affecting the system that require planning and coordination with [to include chief privacy and ISSO and/or similar role or designees] ; and

15. Are reviewed and approved by the authorizing official or designated representative prior to plan implementation.

b. Distribute copies of the plans and communicate subsequent changes to the plans to [to include chief privacy and ISSO and/or similar role];

c. Review the plans [at least annually];

d. Update the plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments; and

e. Protect the plans from unauthorized disclosure and modification.

|  |
| --- |
| **PL-2 Control Summary Information** |
| Responsible Roles: Azure Compliance |
| Parameter pl-02\_odp.01: Azure ISSO, Azure Program Manager |
| Parameter pl-02\_odp.02: Azure ISSO, Azure Program Manager |
| Parameter pl-02\_odp.03: at least annually |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **PL-2 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  The customer is responsible for developing a system security plan (SSP) that meets the criteria defined by the target authorization. Customers may reference NIST Special Publication 800-18 Revision 1, Guide for Developing Security Plans for Federal Information Systems. The customer SSP should address controls inherited from Azure and refer to the Azure SSP for implementation details.  **Azure**  The Azure System Security Plan provides an overview of the security requirements for Azure and the services within. Additionally, it contains a description of the security controls that are in place to meet those requirements.  The Azure System Security Plan is created in accordance with NIST Special Publication 800-18 Revision 1, Guide for Developing Security Plans for Federal Information Systems based on the required template, which contains guidance on security planning. This includes accurately defining the Azure accreditation boundary, as well as describing the operational environment, the security controls that are applicable to the system, and the system interconnections.  The Azure System Security Plan documents the security categorization of the system based on the typical information being stored, processed or transmitted in Azure. The sponsor's Authorizing Official (AO) approves the System Security Plan as part of the package submission and granting of the Authority to Operate (ATO). This SSP:  \* Explicitly defines the boundary of the system in sections 9 and 10 of this document.  \* Provides an overview of the security and operational requirements for the system and a description of the security controls in place or planned for meeting those requirements in the Minimum Security Controls in section 13 of this document.  \* Provides the overview of the infrastructure for storage that provides customers the capability to purchase, use, and/or deploy these offerings within Azure in sections 9 and 10. Customers configure their implementation of Storage using the Azure portal.  \* Provides a security categorization of the system in section 2 based on the information being stored, processed, and transmitted. The system security categorization determination is based on the actual data stored, processed or transmitted by customers utilizing Azure services.  \* Is aligned with the guidance contained in NIST Special Publication 800-18 Revision 1, which contains guidance on security planning. This includes accurately defining Azure, as well as describing the operational environment and all security controls that are applicable to the system.  \* Describes relationships with or connections to other information systems.  \* Is reviewed and approved by the FedRAMP JAB, DISA/DoD authorizing officials, and other regulators prior to plan implementation.  The Microsoft Security Policy (MSP) and associated standards establishes coordination requirements among organizations in order to determine if security and privacy related activities are going to affect Azure. Azure personnel plan and coordinate security and privacy related activities to ensure they do not adversely affect operations. Key operating personnel from each service team assist with change control board and policy reviews that relate to security activities. Individuals assigned to these roles understand the significance of the ongoing security and privacy related activities (security assessments, audits, system hardware and software maintenance, vulnerability scanning and patching, security certifications, and testing exercises), the potential impact on the system, and the necessary support for such activities. If activities involve Azure fundamental services, those teams are included in planning as well. Azure has a formal technology strategy that is maintained and updated annually to align the strategy with business goals and objectives. Azure plans and coordinates security and privacy related activities such as application and infrastructure upgrades, security audits and testing, and continuity planning exercises affecting the information system with C+AI Security management before conducting such activities in order to reduce the impact on organizational operations, organizational assets, individuals, and Azure customers. |
| **Part B**  **Customer Responsibility**  The customer is responsible for distributing the system security plan.  **Azure**  The Azure System Security Plan is posted on the internal Azure SharePoint and distributed to the Azure ISSO and Azure Program Managers. |
| **Part C**  **Customer Responsibility**  The customer is responsible for reviewing the system security plan.  **Azure**  Microsoft works with service teams to review the Azure System Security Plan on an annual basis or when there is a major change to the system at a minimum. Microsoft coordinates these reviews to address changes to the Azure security implementations or problems identified during plan implementation or security control assessments.  In addition to the formal update process, the Azure Compliance team regularly updates the SSP with internal and external customer feedback, process updates, and service improvements. |
| **Part D**  **Customer Responsibility**  The customer is responsible for updating the system security plan.  **Azure**  Microsoft makes updates to the Azure System Security Plan as service teams make changes to the Azure security implementations or the Azure environment to ensure the plan represents an accurate depiction of the Azure security posture. Microsoft coordinates and updates the plan to address changes to the Azure cloud or the network or problems identified during plan implementation or security control assessments. Microsoft formally updates the Azure SSP annually via submission to the regulator. This regulator submission includes upload and maintenance of any regulator Assessment and Authorization (A&A) tooling, including eMASS, Xacta, RSA Archer, CSAM, and more.  In addition to the formal update process, the Azure Compliance team regularly updates the SSP with internal and external customer feedback, process updates, and service improvements. |
| **Part E**  **Customer Responsibility**  The customer is responsible for protecting the system security plan.  **Azure**  The System Security Plan is posted on the internal Azure SharePoint and protected using SharePoint’s built-in confidentiality and integrity protection mechanisms. This SharePoint is used for dissemination only to Azure personnel and relevant external parties. |

## PL-4 Rules of Behavior

a. Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy;

b. Receive a documented acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the system;

c. Review and update the rules of behavior [at least annually] ; and

d. Require individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge [Selection (OneOrMore): [frequency for individuals to read and re-acknowledge the rules of behavior is defined (if selected);] ;when the rules are revised or updated] .

|  |
| --- |
| **PL-4 Control Summary Information** |
| Responsible Roles: HR, Training |
| Parameter pl-04\_odp.01: at least annually |
| Parameter pl-04\_odp.02: at least annually and when the rules are revised or changed |
| Parameter pl-04\_odp.03: |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **PL-4 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  The customer is responsible for establishing rules of behavior.  **Azure**  Microsoft establishes and makes readily available to all Microsoft personnel the Microsoft Acceptable Use Standard which describes Microsoft internal user responsibilities and outlines the Online Services specific acceptable usage standards of the Infrastructure and Services technology assets. The agreements are put in place to protect trade secrets, sensitive, or business confidential information and assets.  Additionally, the Microsoft Security Program Policy (MSPP) describes Microsoft user responsibilities and establishes expected behavior when using Azure and other Microsoft services. All Microsoft personnel, including FTEs, vendors, and contingent staff are required to follow the rules of behavior, which are outlined in the Microsoft Security Program Policy (MSPP) that describes user responsibilities and establishes expected behavior when using Azure and Microsoft services.  The Employee Agreement, the new hire orientation process, and the Microsoft Security Policy (MSP) include statements regarding information and asset protection responsibilities. They also describe the penalties for the violation of these responsibilities. Also communicated via training, Microsoft Services’ security responsibilities extend outside of the work site, beyond the standard operating hours of their employment, and these responsibilities continue for a defined period after employment ends.  All Azure personnel are required to sign and Employee Agreement, as well as other paperwork acknowledging training provided in the new hire orientation process, as a condition for employment. All Azure personnel must provide a signed confirmation indicating understanding and agreement of these expectations prior to gaining access to the Microsoft’s network.  The annual fulfillment of the Security Foundations Training is signed by all personnel and meets the requirements for the rules of behavior and access agreements. At the end of the Security Foundations Training, the personnel must check a box acknowledging that they have access to the Microsoft Policy and will abide by those policies. All personnel also must take the Standards of Business Conduct (SBC) training, which includes additional information on responsibilities. |
| **Part B**  **Customer Responsibility**  The customer is responsible for obtaining signed acknowledgment of the rules of behavior from system users.  **Azure**  In accordance with the Microsoft Security Policy, Microsoft requires signed acknowledgment from personnel indicating that they have read, understand, and agree to abide by user requirements before gaining authorized access to Azure.  All Azure personnel are required to sign an Employee Agreement with non-disclosure provisions, as well as acknowledging security training provided in the new hire orientation process, at the time of hiring as a condition for employment. This signature acknowledges the terms and conditions of their role and their understanding and acceptance of the Microsoft corporate policies (including the Microsoft Security Program Policy (MSPP)). Contingent staff members (vendors and subcontractors) are required to sign and acknowledge the Microsoft Resource Access Agreement prior to being granted access to Microsoft information and services. Additionally, contingent staff members inherit the responsibilities based on the agreement between Microsoft and their respective organizations as detailed in respective contracts. All Azure personnel are also required to sign an Employee Agreement. |
| **Part C**  **Customer Responsibility**  The customer is responsible for reviewing and updating the rules of behavior.  **Azure**  Microsoft reviews the Non-Disclosure Agreement, the Microsoft Security Policy and other contractual paperwork signed during the new hire orientation process at least annually. If changes are needed, Microsoft updates the paperwork during the annual review. The paperwork is updated in an annual basis.  On an annual basis, Microsoft employees are required to review the rules of behavior through the annual Security Foundations training. Personnel signature is evidenced through the successful completion of the security training which requires in-course attestation. The security training which includes the rules of behavior is updated annually. |
| **Part D**  **Customer Responsibility**  The customer is responsible for obtaining signed acknowledgment of the updated rules of behavior from system users.  **Azure**  After revisions, the revised document is included in annual security awareness training, which all personnel must take and sign upon completion. |

### PL-4(1) - Social Media and External Site/Application Usage Restrictions

Include in the rules of behavior, restrictions on:

(a) Use of social media, social networking sites, and external sites/applications;

(b) Posting organizational information on public websites; and

(c) Use of organization-provided identifiers (e.g., email addresses) and authentication secrets (e.g., passwords) for creating accounts on external sites/applications.

|  |
| --- |
| **PL-4(1) Control Summary Information** |
| Responsible Roles: HR, Training |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **PL-4(1) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for including restrictions on the use of social media/networking sites, posting organizational information on public websites in the rules of behavior, and using of customer-provided identifiers for creating account on external sites/applications.  **Azure**  The Standards of Business Conduct (SBC) training includes explicit restrictions on the use of social media/networking sites and posting organizational information on public websites. The Standards of Business Conduct (SBC) training course is taken by all Azure employees on an annual basis.  Azure documentation posted on Microsoft owned public websites is restricted to Azure personnel via Microsoft identities. Azure personnel who own pieces of Azure documentation have the Microsoft identity credentials to provision access and post Azure content. |

## PL-8 Security and Privacy Architectures

a. Develop security and privacy architectures for the system that:

1. Describe the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information;

2. Describe the requirements and approach to be taken for processing personally identifiable information to minimize privacy risk to individuals;

3. Describe how the architectures are integrated into and support the enterprise architecture; and

4. Describe any assumptions about, and dependencies on, external systems and services;

b. Review and update the architectures [at least annually and when a significant change occurs] to reflect changes in the enterprise architecture; and

c. Reflect planned architecture changes in security and privacy plans, Concept of Operations (CONOPS), criticality analysis, organizational procedures, and procurements and acquisitions.

(b) Guidance: Significant change is defined in NIST Special Publication 800-37 Revision 2, Appendix F.

|  |
| --- |
| **PL-8 Control Summary Information** |
| Responsible Roles: Azure Compliance |
| Parameter pl-8(b): at least annually and when a significant change occurs |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **PL-8 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for developing an information security and privacy architecture for customer-deployed resources.  **Azure**  Azure’s security and privacy architecture describes:  \* The overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of data relevant to and stored within Azure  \* Standards in place to process personally identifiable information to minimize privacy risk  \* The integration of Azure architecture into Azure’s Infrastructure architecture  \* Assumptions about and dependencies on external services  Guidance for the development of the information system architecture for Azure is included in the Microsoft Security Program Policy (MSPP), MSP-08 Operations Security.  **Documented Operating Procedures, Service Architecture, and Threat Modeling**  Operating procedures for services providing Microsoft’s services must also be formally documented, approved, and communicated and should contain, at a minimum, those processes that impact the confidentiality, integrity, or availability of a system and critical data. Service architecture must be documented and threat modeling is performed to identify security threats to the service and ensure adequate mitigations are in place. System operations staff must develop Security configuration baseline for services and ensure that services are implemented according to approved security configuration baseline.  **Antivirus and Anti-Malware Protection**  All Microsoft services must be protected from malicious software and hardware. Microsoft personnel are made aware of the potential dangers resulting from circumvention of network controls, such as downloading files from unknown or untrusted sources or providing inappropriate access. Security incidents that occur must be logged, verified, retained, secured, and appropriate corrective actions must be taken in response to these events.  **Security Logging, Monitoring, and Reporting**  System operations staff must implement monitoring technology and/or procedures to ensure timely detection and response to security incidents. Audit logs must be examined in a timely manner, and all identified anomalies must be investigated for possible misuse or compromise. Any log event which indicates a potential violation of Microsoft’s Security Policy must be brought to the attention of the respective organization’s appropriate service team.  System operations staff ensure key services must have appropriate logging enabled and securely transmit logs to a central collection point. Logs must be maintained for a specified period of time according to standards. Monitoring and reporting tools must be available and used to assess the security posture of Microsoft.  **Change Control and Acceptance**  An operational change control procedure must be in place for each operational service team within Microsoft. These procedures must include a process for organizational management review and approval. These change control procedures must be communicated to all parties (Microsoft and third parties) who perform system maintenance on or in any of Microsoft’s facilities.  Acceptance criteria must be established by each security organization for new services, upgrades to existing services, and changes to processes to ensure services meet this security policy and any associated procedures and standards.  **Security Vulnerabilities and Penetration Testing**  To help prevent the risk of exposure to known security vulnerabilities, it is the responsibility of each Asset Owner to ensure their services have the latest security related patches. Systems operations staff must proactively monitor the service assets for possible exposures. This monitoring must include scanning for known system vulnerabilities and penetration testing from outside as well as inside Microsoft’s environment. These activities must be scheduled and conducted in such a fashion as to minimize impact to the environment or organization. The frequency of scanning and penetration testing is determined by the sensitivity and criticality of the system. |
| **Part B**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for reviewing and updating the information security architecture.  **Azure**  Azure reviews and updates the information security architecture annually and when significant changes are made to Azure architecture or changes are made within the Microsoft Security Program Policy (MSPP). |
| **Part C**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for accounting for planned changes to the information security architecture.  **Azure**  Azure updates this System Security Plan and all Azure procurement/acquisition procedures annually or whenever the information security architecture changes. |

## PL-10 Baseline Selection

Select a control baseline for the system.

Requirement: Select the appropriate FedRAMP Baseline

|  |
| --- |
| **PL-10 Control Summary Information** |
| Responsible Roles: Azure Compliance |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **PL-10 What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for selecting control baseline for customer-deployed resources.  **Azure**  Azure implements NIST 800-53 rev 5 security control baselines that have been selected by FedRAMP Program Management Office (PMO) to support FedRAMP High compliance requirements and by United States DoD regulators to support DoD SRG compliance requirements. . Azure employs an approved Third-Party Assessment Organization (3PAO) as an independent assessor to conduct a security control assessment of Azure in accordance with security control requirements. The results of this assessment and related activities are submitted to Azure’s authorizing officials. |

## PL-11 Baseline Tailoring

Tailor the selected control baseline by applying specified tailoring actions.

|  |
| --- |
| **PL-11 Control Summary Information** |
| Responsible Roles: Azure Compliance |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **PL-11 What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for tailoring selected control baseline by applying specified tailoring actions for customer-deployed systems.  **Azure**  Azure implements NIST 800-53 rev 5 security control baselines that have been selected by FedRAMP Program Management Office (PMO) to support FedRAMP High compliance requirements and by United States DoD regulators to support DoD SRG compliance requirements. . Azure designs and tailors processes around the security controls where sprit of the controls are addressed by taking mitigation actions on identified risks. Azure employs an approved Third-Party Assessment Organization (3PAO) as an independent assessor to conduct a security control assessment of Azure in accordance with security control requirements. The results of this assessment and related activities are submitted to Azure’s authorizing officials. |

# Personnel Security (PS)

## PS-1 Policy and Procedures

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (OneOrMore): organization-level;mission/business process-level;system-level] personnel security policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the personnel security policy and the associated personnel security controls;

b. Designate an [an official to manage the personnel security policy and procedures is defined;] to manage the development, documentation, and dissemination of the personnel security policy and procedures; and

c. Review and update the current personnel security:

1. Policy [at least annually] and following [events that would require the current personnel security policy to be reviewed and updated are defined;] ; and

2. Procedures [at least annually] and following [significant changes].

|  |
| --- |
| **PS-1 Control Summary Information** |
| Responsible Roles: SOP Team, Policy |
| Parameter ps-1(a): all personnel |
| Parameter ps-01\_odp.01: |
| Parameter ps-01\_odp.02: |
| Parameter ps-01\_odp.03: a Microsoft-wide |
| Parameter ps-01\_odp.04: the Microsoft Information Risk Management Council (IRMC) organization |
| Parameter ps-01\_odp.05: at least annually |
| Parameter ps-01\_odp.06: significant changes |
| Parameter ps-01\_odp.07: at least annually |
| Parameter ps-01\_odp.08: significant changes |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☒ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **PS-1 What is the solution and how is it implemented?** |
| **Part A1**  **Customer Responsibility**  The customer is responsible for developing, documenting, and disseminating personnel security policy and procedures that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.  **Azure**  Azure addresses the personnel security policy as part of the Microsoft security policies, of which there are two sets: the Microsoft Security Policy (MSP) that is applicable to all Microsoft personnel, and the Microsoft Security Program Policy (MSPP), which is applicable to all Microsoft personnel that have a responsibility for security. The Microsoft Information Risk Management Council (IRMC) is the governance body with review and approval responsibility for the MSP and MSPP. Within Azure, the MSPP specifically applies to all with security objectives such as, Microsoft personnel with security objectives such as designing, building, and operating Azure and across all information and processes used in the conduct of Microsoft business. All Azure personnel are accountable and responsible for complying with these guiding principles within their designated roles. The policy addresses the following:  \* Personnel screening  \* Personnel security  Additionally, the policy addresses the purpose, scope, roles, responsibilities, compliance requirements, and required coordination among the various Microsoft organizations that provide some level of support to all services. The policies indicate Microsoft management’s commitment and are a component of the risk management strategy which provides Azure personnel with a current set of clear and concise information security requirements.  The MSP is available to all Microsoft personnel on the Microsoft Policy website on the Microsoft intranet, and the MSPP and Security Standards are available through the Liquid tool, also on the Microsoft intranet. The Azure SOPs are stored in the Azure Security, Privacy & Compliance SharePoint site. This SharePoint site is accessible to all Azure personnel.  Service teams may supplement the Azure policies and procedures with offering-specific policies and procedures. Service-team-specific policies and procedures associated with personnel security are documented and stored within internal Azure SharePoint sites. Only personnel with authorized credentials, adequate levels of permission, legitimate need to know, and specific roles and responsibilities are given access to the service-team-specific policies or procedures. |
| **Part A2**  **Customer Responsibility**  The customer is responsible for procedures to facilitate the implementation of the personnel security policy and the associated personnel security controls.  **Azure**  The Azure Personnel Screening Standard Operating Procedure (SOP) implements the personnel security policy and associated controls and documents the following procedures:  \* Background checks  \* References  \* Screening requirements  Service teams may supplement the Azure policies and procedures with offering-specific policies and procedures. Service-team-specific policies and procedures associated with personnel security are documented and stored within internal Azure SharePoint sites. Only personnel with authorized credentials, adequate levels of permission, legitimate need to know, and specific roles and responsibilities are given access to the service-team-specific policies or procedures. |
| **Part B**  **Customer Responsibility**  The customer is responsible for designating an official to manage the development, documentation, and dissemination of personnel security planning policy and procedures.  **Azure**  The Microsoft Information Risk Management Council (IRMC) organization is the governance body with approval responsibility for the Microsoft Security Policy (MSP) and Microsoft Security Program Policy (MSPP). The IRMC consists of representatives from security and risk management teams across Microsoft including Core Services Engineering and Operations (CSEO), Azure, and Global Security. The Customer Security and Trust: Security Engineering (CST-SE) organization manages the review and approval process and maintains the policies.  On an annual basis, the CST-SE conducts a line-by-line review of the MSP and MSPP. The Microsoft Security Policy (MSP) and Microsoft Security Program Policy (MSPP) Governance document describes each member’s role, types and frequency of review, escalation paths, approval process, and formal publishing procedures of the security policy. Throughout the year, if necessary, CST-SE may convene with the IRMC to conduct reviews after a significant review or change request. The approved policy update is published within the relevant tool on the Microsoft intranet. If service teams establish service-specific or team-specific policies, the respective service teams update the necessary policies at least annually. |
| **Part C1**  **Customer Responsibility**  The customer is responsible for reviewing and updating the current personnel security policy on a regular basis and following organization-defined events.  **Azure**  The Azure team updates the Azure SOPs at least annually through a formal review process. If needed, the Azure team updates the SOP after a significant change affecting policy execution as well. If established, service-team-specific procedures are updated by their respective teams. The individual service teams review and update their respective SOPs at least annually and when required by a significant change. |
| **Part C2**  **Customer Responsibility**  The customer is responsible for reviewing and updating the current personnel security procedures on a regular basis and following organization-defined events.  **Azure**  The Azure team updates the Azure SOPs at least annually through a formal review process. If needed, the Azure team updates the SOP after a significant change affecting policy execution as well. If established, service-team-specific procedures are updated by their respective teams. The individual service teams review and update their respective SOPs at least annually and when required by a significant change. |

## PS-2 Position Risk Designation

a. Assign a risk designation to all organizational positions;

b. Establish screening criteria for individuals filling those positions; and

c. Review and update position risk designations [at least annually].

|  |
| --- |
| **PS-2 Control Summary Information** |
| Responsible Roles: CELA, Personnel Screening |
| Parameter ps-2(c): At least annually |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **PS-2 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  The customer is responsible for assigning risk designations to positions.  **Azure**  Microsoft ensures that all Azure personnel including subcontractors have risk designations in place based on role assignments. The risk designation is based on the asset classification assigned to information accessed, including federal customer data. Asset classification is determined through the types of information the asset contains. |
| **Part B**  **Customer Responsibility**  The customer is responsible for establishing screening criteria to screen individuals filling the positions identified in PS-02 Part a.  **Azure**  Azure, in coordination with Microsoft Human Resources (HR), establishes screening criteria for Azure service team personnel by reviewing positions for risk as well as considering customer expectations. All personnel require the Microsoft Cloud Screen. |
| **Part C**  **Customer Responsibility**  The customer is responsible for reviewing and updating risk designations on a customer-defined frequency.  **Azure**  Microsoft reviews the position risk designations as part of the annual Personnel Screening Standard Operating Procedure (SOP) update. All positions are subject to screening requirements. |

## PS-3 Personnel Screening

a. Screen individuals prior to authorizing access to the system; and

b. Rescreen individuals in accordance with [for national security clearances; a reinvestigation is required during the fifth (5th) year for top secret security clearance, the tenth (10th) year for secret security clearance, and fifteenth (15th) year for confidential security clearance. For moderate risk law enforcement and high impact public trust level, a reinvestigation is required during the fifth (5th) year. There is no reinvestigation for other moderate risk positions or any low risk positions].

|  |
| --- |
| **PS-3 Control Summary Information** |
| Responsible Roles: CELA, Personnel Screening |
| Parameter ps-3(b): As defined by customer; there are no reinvestigation requirements for moderate and low public trust positions |
| Parameter ps-03\_odp.01: |
| Parameter ps-03\_odp.02: |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **PS-3 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  The customer is responsible for screening individuals prior to authorizing access to customer-deployed resources.  **Azure**  Microsoft Security conducts background checks and enforces the screening policies for all personnel. Background checks in the form of the Microsoft Cloud Screen are required for new hires or personnel transferring to positions that involve access to customers’ work sites and/or sensitive areas, including access to customer PII.  The Microsoft Cloud Screen includes the following:  \* Employment history check for the previous five years  \* Education Check (highest degree obtained)  \* Social Security Number (SSN) Check  \* Criminal History Check for the previous seven years  \* Office of Foreign Assets Control List (OFAC) Check  \* Bureau of Industry and Security List (BIS) Check  \* Office of Defense Trade Controls Debarred Persons List Check  Vendor staff with access to customer data are required to sign a background screening addendum with Microsoft or provide the results of the background screening from the third-party provider. Microsoft managers are required to include screening verbiage in their respective SOWs with vendors. |
| **Part B**  **Customer Responsibility**  The customer is responsible for re-screening individuals at a customer-defined frequency or under customer-defined conditions.  **Azure**  This control is not applicable. Background investigation requirements for Azure for FedRAMP are only at the Minimum Background Investigation level, and there are no reinvestigation requirements for moderate and low public trust positions. |

### PS-3(3) - Information Requiring Special Protective Measures

Verify that individuals accessing a system processing, storing, or transmitting information requiring special protection:

(a) Have valid access authorizations that are demonstrated by assigned official government duties; and

(b) Satisfy [personnel screening criteria - as required by specific information].

|  |
| --- |
| **PS-3(3) Control Summary Information** |
| Responsible Roles: CELA, Personnel Screening |
| Parameter ps-03.03\_odp: Screening criteria established in PS-03 |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **PS-3(3) What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  The customer is responsible for controlling access to protected information by verifying that individuals accessing customer-deployed resources which process, store, or transmit information requiring special protection have been assigned official government duties that demonstrate valid access authorizations.  **Azure**  Azure personnel are required to satisfy the screening requirements. |
| **Part B**  **Customer Responsibility**  The customer is responsible for controlling access to protected information by ensuring that individuals accessing customer-deployed resources which process, store, or transmit information requiring special protection, satisfy any additional customer-defined personnel screening criteria.  **Azure**  Azure personnel are required to satisfy the screening requirements. |

## PS-4 Personnel Termination

Upon termination of individual employment:

a. Disable system access within [one (1) hour];

b. Terminate or revoke any authenticators and credentials associated with the individual;

c. Conduct exit interviews that include a discussion of [information security topics to be discussed when conducting exit interviews are defined;];

d. Retrieve all security-related organizational system-related property; and

e. Retain access to organizational information and systems formerly controlled by terminated individual.

|  |
| --- |
| **PS-4 Control Summary Information** |
| Responsible Roles: JIT, OneIdentity, HR, CELA |
| Parameter ps-04\_odp.01: four (4) hours |
| Parameter ps-04\_odp.02: non-disclosure agreements and the exit process |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **PS-4 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  The customer is responsible for appropriately terminating customer personnel within a customer-defined time period.  **Azure**  Microsoft HR and Azure management ensure personnel termination is handled appropriately. For voluntary terminations, on the last day of employment, the individual is terminated from the HR system via a Termination Transaction ticket entered in the Employee/Manager Self Service Tool by the employee, manager, group administrator, or equivalent personnel with work-on-behalf privileges. For involuntary terminations, the request is submitted by the aligned HR Employee Relations Manager to the Central HR Operations team for processing.  Once entered, voluntary termination requests are approved by the individual’s manager, group administrator, or equivalent personnel with work-on-behalf privileges. Once the transaction has been entered and approved, Microsoft Accounts and Security teams are notified and access to services is disabled. Human Resources is also notified of the termination request. For voluntary terminations, access is disabled on the last day of employment, barring any special considerations such as security concerns or if the employee is leaving for a competitor. For involuntary terminations, an urgent request for access termination is submitted via email from HR and access is disabled within four (4) hours.  Terminations are communicated to personnel required to remove information system and physical access to facilities via the Employee Central (EC) termination transaction process and/or urgent terminations email template. The supervisor or/and Business Administrators are responsible for ensuring that all local access to Azure physical components is removed. |
| **Part B**  **Customer Responsibility**  The customer is responsible for the appropriate revocation of authenticators/credentials associated with terminated customer personnel.  **Azure**  When an individual is terminated via voluntary termination, he or she is removed from the Human Resources Information System (HRIS) via a Termination Transaction approved by the individual’s manager, group administrator, or equivalent personnel with work-on-behalf privileges. If an individual is involuntarily terminated, the request is submitted by the central HR Operations team via a request from the org-aligned HR Manager. When an individual is marked as terminated in HRIS, this information propagates to Active Directory, which then automatically removes/revokes any authenticators/credentials associated with the individual. |
| **Part C**  **Customer Responsibility**  The customer is responsible for conducting exit interviews which include customer-defined information security topics upon termination of customer personnel.  **Azure**  Microsoft sends an exit survey personnel being hired by a competitor on or before the user’s last day at Microsoft. Topics covered in the exit survey include review of Employee Agreement provisions. Exit survey may not be conducted in the event of a termination where the individual is not going to a competitor. |
| **Part D**  **Customer Responsibility**  The customer is responsible for retrieving all security- and system-related property upon termination of customer personnel.  **Azure**  Upon termination, building access smart cards, logical access smart cards, computer/hardware, and vehicle authorization tags are collected. Access to the work location, office, or station is denied or supervised to allow the individual to gather personal belongings prior to being escorted out of the building. These processes ensure that Microsoft collects all security-related, organizational information system-related property prior to the terminated individual’s departure. |
| **Part E**  **Customer Responsibility**  The customer is responsible for retaining access to resources formally controlled by terminated customer personnel.  **Azure**  Microsoft retains information formerly controlled by terminated individual on file servers and SQL/SharePoint as part of the Data Protection Services’ (DPS) disaster recovery retention for ninety (90) days. Additionally, managers can also gain access to workstations of terminated personnel after HR has approved the requested access. |

### PS-4(2) - Automated Actions

Use [automated mechanisms to notify personnel or roles of individual termination actions and/or to disable access to system resources are defined;] to [Selection (OneOrMore): notify [personnel or roles to be notified upon termination of an individual is/are defined (if selected);] of individual termination actions;disable access to system resources] .

|  |
| --- |
| **PS-4(2) Control Summary Information** |
| Responsible Roles: JIT, OneIdentity, HR |
| Parameter ps-04.02\_odp.01: organization-defined automated mechanisms |
| Parameter ps-04.02\_odp.02: Access control personnel responsible for disabling access to the system |
| Parameter ps-04.02\_odp.03: |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **PS-4(2) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for employing automated mechanisms to notify customer-defined personnel/roles upon termination of a customer employee.  **Azure**  Microsoft Human Resources (HR) and the individual’s manager ensure personnel termination is handled appropriately. The individual is terminated from the HR system via a Termination Transaction ticket entered in the Manager Self Service Tool and approved by the individual’s manager, group administrator, or equivalent personnel with work-on-behalf privileges. Once the transaction has been entered and approved, Microsoft Accounts and Security teams are notified and access to services and physical locations is disabled. |

## PS-5 Personnel Transfer

a. Review and confirm ongoing operational need for current logical and physical access authorizations to systems and facilities when individuals are reassigned or transferred to other positions within the organization;

b. Initiate [transfer or reassignment actions to be initiated following transfer or reassignment are defined;] within [twenty-four (24) hours];

c. Modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and

d. Notify [including access control personnel responsible for the system] within [twenty-four (24) hours].

|  |
| --- |
| **PS-5 Control Summary Information** |
| Responsible Roles: JIT, OneIdentity, HR |
| Parameter ps-05\_odp.01: reassignment of access to data |
| Parameter ps-05\_odp.02: within twenty-four (24) hours of an employee transferring to a new position with new reporting structures of cost centers |
| Parameter ps-05\_odp.03: transferring personnel's manager |
| Parameter ps-05\_odp.04: twenty-four (24) hours |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **PS-5 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  The customer is responsible for appropriately transferring personnel and reviewing current logical and physical access authorizations to customer-deployed resources/facilities when individuals are reassigned or transferred.  **Azure**  Microsoft HR ensures personnel transfer is handled appropriately. Microsoft implements personnel transfer using the Manager Self Service Tool, which is managed by Microsoft Headcount Operations. When personnel transfer to new positions with new reporting structures, a Manager Self Service Tool transfer transaction is keyed into the HR system by the individual’s manager, group administrator, or equivalent personnel with work-on-behalf privileges. Once the transfer has populated in the downstream tools and applications, access to data is reassigned based on the new role and scope within twenty-four (24) hours of transfer.  Access to buildings, rooms, and websites can be requested by the transferred individual’s manager. |
| **Part B**  **Customer Responsibility**  The customer is responsible for performing customer-defined actions that must be taken within a defined time period following formal transfer/reassignment of customer personnel.  **Azure**  Azure ensures account management activities associated with personnel transfer is initiated within twenty-four (24) hours of submission for personnel who are reassigned or transferred to other positions within the organization. |
| **Part C**  **Customer Responsibility**  The customer is responsible for modifying access authorizations of transferred/reassigned customer personnel because of the review performed in PS-05 Part a.  **Azure**  Microsoft HR ensures personnel transfer is handled appropriately. Microsoft implements personnel transfer using the Manager Self Service Tool, which is managed by Microsoft Headcount Operations. When personnel transfer to new positions with new reporting structures, the Manager Self Service Tool transfer transaction is keyed into the HR system by the individual’s manager, group administrator, or equivalent personnel with work-on-behalf privileges. Once the transfer has populated in the downstream tools and applications, access to data is reassigned based on the new role and scope within twenty-four (24) hours of transfer.  Access to buildings/rooms/websites can be requested by the transferred individual’s manager. |
| **Part D**  **Customer Responsibility**  The customer is responsible for notifying customer-defined personnel/roles within a customer-defined time period following customer personnel transfer/ reassignment.  **Azure**  Microsoft Managers of employees are responsible for ensuring personnel transfer is initiated within twenty-four (24) hours for personnel who are reassigned or transferred to other positions within the organization in the Employee Central system. Subsequently, the new managers of employees are responsible to approve the initiated request in the Employee Central system. Microsoft defines the transfer or reassignment actions to implement using the Employee Central system, which is managed by Microsoft Human Resources. When an individual transfers to a position within a different cost center, an Employee Central transfer transaction is keyed into system by HR Operations. |

## PS-6 Access Agreements

a. Develop and document access agreements for organizational systems;

b. Review and update the access agreements [at least annually] ; and

c. Verify that individuals requiring access to organizational information and systems:

1. Sign appropriate access agreements prior to being granted access; and

2. Re-sign access agreements to maintain access to organizational systems when access agreements have been updated or [at least annually and any time there is a change to the user's level of access].

|  |
| --- |
| **PS-6 Control Summary Information** |
| Responsible Roles: HR, Training, CELA |
| Parameter ps-06\_odp.01: At least annually |
| Parameter ps-06\_odp.02: At least annually and any time there is a change to the user's geographic location |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **PS-6 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  The customer is responsible for developing and documenting access agreements for customer-deployed resources.  **Azure**  Microsoft has developed and documented confidentiality and non-disclosure provisions for personnel requiring access to Azure in various roles.  Before gaining access to services, Microsoft full time employees (FTEs) must sign the Employee Agreement which includes non-disclosure provisions and statements regarding information and asset protection responsibilities. This document also describes the penalties for the violation of these responsibilities. The annual fulfillment of the Security Foundations Training course is signed by the employee and meets the requirements for the rules of behavior and access agreements. At the end of the Security Foundations Training, the employee must check a box acknowledging that the employee has access to the Microsoft Policy and that the employee will abide by those policies.  Third parties, such as subcontractors and vendors, must complete the Resource Access Agreements which includes non-disclosure provisions and statements regarding information and asset protection responsibilities.  In addition, all Microsoft employees are required to sign paperwork acknowledging security training provided during the new hire orientation process. During this training, descriptions are given as to the responsibilities and expected behavior regarding information and information system usage. It is also communicated that security responsibilities extend outside of the work site and beyond the standard operating hours of their employment and continues for a defined period after employment ends. It is the duty of Microsoft personnel to comply with regulatory mandates. |
| **Part B**  **Customer Responsibility**  The customer is responsible for reviewing and updating access agreements at a customer-defined frequency.  **Azure**  The Employee Agreement, Resource Access Agreement, and other contractual documents signed as part of the new hire orientation process, are reviewed annually to reflect changes in the Microsoft environment, and updated on an as-needed basis. |
| **Part C1**  **Customer Responsibility**  The customer is responsible for verifying that individuals requiring access to customer-deployed resources review and sign access agreements prior to being granted access.  **Azure**  Prior to granting access to organizational information and services, all Microsoft full-time employees (FTEs) must sign the Employee Agreement as a condition of employment.  Third parties, such as subcontractors and vendors, must complete the Resource Access Agreements which includes non-disclosure provisions and statements regarding information and asset protection responsibilities. |
| **Part C2**  **Customer Responsibility**  The customer is responsible for verifying that individuals requiring access to customer-deployed resources re-sign when the agreements have been updated and/or at a customer-defined frequency.  **Azure**  Employees resign the EA if they move to some geographic locations. Submission of annual training completion constitutes agreement that the user understands and agrees to the EA.  Third parties, such as subcontractors and vendors, must complete the Resource Access Agreements which includes non-disclosure provisions and statements regarding information and asset protection responsibilities. Third parties are also required to take Supplier Code of Conduct training (SCOC).  Because of the nature of JIT access, a user’s level of access can change multiple times per day. As such, Azure does not require resigning of the EA or retraining any time there is a change to the user's level of access. |

## PS-7 External Personnel Security

a. Establish personnel security requirements, including security roles and responsibilities for external providers;

b. Require external providers to comply with personnel security policies and procedures established by the organization;

c. Document personnel security requirements;

d. Require external providers to notify [including access control personnel responsible for the system and/or facilities, as appropriate] of any personnel transfers or terminations of external personnel who possess organizational credentials and/or badges, or who have system privileges within [terminations: immediately; transfers: within twenty-four (24) hours] ; and

e. Monitor provider compliance with personnel security requirements.

|  |
| --- |
| **PS-7 Control Summary Information** |
| Responsible Roles: HR |
| Parameter ps-07\_odp.01: The third-party provider's Microsoft FTE manager |
| Parameter ps-07\_odp.02: Terminations: immediately; transfers: within twenty-four (24) hours |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **PS-7 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  The customer is responsible for third-party personnel security.  **Azure**  Personnel security requirements, including security roles and responsibilities for third-party providers, are established by requiring them to comply with the Microsoft Security Policy (MSP). This includes personnel located at Microsoft subsidiaries and locations not owned by Microsoft, such as off-site facilities. Any third-party personnel with access to Azure must pass the same personnel screening process for the requirements established for the risk categorization of their role.  In all contracts, Microsoft includes provisions to ensure that third-party providers meet or exceed the personnel security requirements mandated by Microsoft. This includes the ability to successfully pass the Microsoft background check, or equivalent, as well as obtain and maintain additional clearances if the specific project requires it. Third-party providers that have access to the are subject to the same personnel screening requirements as Microsoft personnel working on Azure services for U.S. Government customers, including Federal background investigations.  Vendors and subcontractors that require logical access to Federal customer data, or physical access to controlled facilities that house Federal customer data (other than on an occasional or intermittent basis) for the Azure service are required to successfully complete Federal adjudicated background investigations.  Should a vendor or subcontractor require physical access to controlled facilities that contain customer data, a cleared/authorized individual is provided as an escort and must accompany the vendor or subcontractor at all times while in the secured location. |
| **Part B**  **Customer Responsibility**  The customer is responsible for requiring third-party providers to comply with customer-defined personnel security policies and procedures.  **Azure**  Microsoft requires vendors and contractors to have a signed contract to ensure compliance with Microsoft policies and procedures, including personnel security policies and procedures, on required engagements. |
| **Part C**  **Customer Responsibility**  The customer is responsible for documenting third-party personnel security requirements defined in PS-07.a.  **Azure**  Personnel security requirements are documented in all vendor contracts and the Addendum to Supplier Agreement (Background Requirements). |
| **Part D**  **Customer Responsibility**  The customer is responsible for requiring third-party providers to notify customer-defined personnel/roles of any transfers/terminations of third-party personnel who possess customer credentials and/or smart cards within a customer-defined period of time.  **Azure**  Microsoft documents third-party security requirements in the Microsoft Security Policy (MSP) and associated standards. Specific notification requirements for transfers and terminations of third-party personnel with access to Azure are identical to those for Microsoft personnel. |
| **Part E**  **Customer Responsibility**  The customer is responsible for third-party personnel security, including monitoring of third-party provider compliance with customer-defined requirements.  **Azure**  Microsoft monitors compliance with screening requirements for third-party personnel by tracking the outcome of screening directly. Microsoft requires approved screening vendors to submit screening outcomes for third-party personnel directly to Microsoft where they are tracked in HRIS and monitored by the groups contracting with the vendor. |

## PS-8 Personnel Sanctions

a. Employ a formal sanctions process for individuals failing to comply with established information security and privacy policies and procedures; and

b. Notify [to include the ISSO and/or similar role within the organization] within [24 hours] when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

|  |
| --- |
| **PS-8 Control Summary Information** |
| Responsible Roles: HR, CELA |
| Parameter ps-08\_odp.01: the employee and employee's manager |
| Parameter ps-08\_odp.02: two weeks of investigation completion |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **PS-8 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  The customer is responsible for establishing a sanctions process for customer employees failing to comply with information security and privacy policies and procedures.  **Azure**  Microsoft’s formal sanctions process for personnel failing to comply with established information security policies and procedures is defined in the Microsoft Security Policy (MSP). Specifically, depending on the particular type of misconduct, Microsoft’s Online Services Staff suspected of committing breaches of security and/or violating Microsoft Security Program Policy (MSPP) are subject to an investigation process and appropriate disciplinary action up to and including termination.  When the Microsoft Human Resources (HR) team is notified of a possible security violation, the Office of Legal Compliance (OLC) is consulted. The OLC team advises HR if it is in scope for their team. If the incident is in scope for OLC, OLC investigates the possible security violation and reconnects with HR and the employee’s manager on the findings. If the allegation is substantiated, OLC recommends the disciplinary action to be taken and directs HR and the employee’s manager to debrief the employee and implement the discipline. Violations of Microsoft Information Security policies, standards, or procedures may result in corrective action, up to and including immediate termination of employment. In some cases, a breach of Microsoft Information Security policies, standards, or procedures may also violate an international, federal, state, or local law. In such cases, the individual may also be subject to civil and/or criminal liability.  Once the OLC findings are delivered to HR and management, the employee, absent extenuating circumstances, is typically debriefed within two (2) weeks. This would be the same if HR were leading the investigation, not in scope for OLC.  Violations that align with NIST Special Publication 800-61 Revision 2, incident categories are reported to US-CERT and the impacted customer agency per the incident reporting requirements. |
| **Part B**  **Customer Responsibility**  The customer is responsible for providing notifications, comprised of the identification of the sanctioned individual and the reason for the sanction, to customer-defined personnel/roles within a customer-defined time period when a formal employee sanctions process is initiated.  **Azure**  Microsoft’s formal sanctions process for personnel failing to comply with established information security policies and procedures is defined in the Microsoft Security Policy (MSP). Specifically, depending on the particular type of misconduct, Microsoft’s Online Services Staff suspected of committing breaches of security and/or violating Microsoft Security Program Policy (MSPP) are subject to an investigation process and appropriate disciplinary action up to and including termination.  When the Microsoft Human Resources (HR) team is notified of a possible security violation, the Office of Legal Compliance (OLC) is consulted. The OLC team advises HR if it is in scope for their team. If the incident is in scope for OLC, OLC investigates the possible security violation and reconnects with HR and the employee’s manager on the findings. If the allegation is substantiated, OLC recommends the disciplinary action to be taken and directs HR and the employee’s manager to debrief the employee and implement the discipline. Violations of Microsoft Information Security policies, standards, or procedures may result in corrective action, up to and including immediate termination of employment. In some cases, a breach of Microsoft Information Security policies, standards, or procedures may also violate an international, federal, state, or local law. In such cases, the individual may also be subject to civil and/or criminal liability.  Once the OLC findings are delivered to HR and management, the employee, absent extenuating circumstances, is typically debriefed within two (2) weeks. This would be the same if HR were leading the investigation, not in scope for OLC.  Security incidents are reported to the customers and US-CERT per the incident reporting requirements. |

## PS-9 Position Descriptions

Incorporate security and privacy roles and responsibilities into organizational position descriptions.

|  |
| --- |
| **PS-9 Control Summary Information** |
| Responsible Roles: HR, Training |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **PS-9 What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for incorporating security and privacy roles and responsibilities into organizational position descriptions for customer-deployed resources.  **Azure**  Microsoft ensures that all Azure personnel including subcontractors have risk designations in place based on role assignments. The risk designation is based on the asset classification assigned to information accessed, including federal customer data. Asset classification is determined through the types of information the asset contains. Azure, in coordination with Microsoft Human Resources (HR), establishes screening criteria for Azure service team personnel by reviewing positions for risk as well as considering customer expectations. All personnel require the Microsoft Cloud Screen. Microsoft reviews the position risk designations as part of the annual Personnel Screening SOP update. All positions are subject to screening requirements. Personnel role assignments have concepts of privacy and security principles backed on them through the following training.  Microsoft C+AI training and awareness components are classified into one of two types for personnel: Role-Based and Required.  Role-Based Training  Role-Based training is mandatory security and awareness education that is deemed helpful in the facilitation of understanding security processes and procedures for a particular role an individual is placed in and is directly related to the job responsibilities of the individual. Role-Based training is offered to full-time personnel through the STRIKE program for engineering disciplines providing 200-400 level security training and best practices.  Required Training  Required training is mandatory security and awareness education that the Information Risk Management Council (IRMC) has specifically identified and defined as appropriate for Azure personnel based upon their organization. Required annual training includes Security Foundations for new hires and non-engineering FTEs and the STRIKE program for engineering FTEs. |

# Risk Assessment (RA)

## RA-1 Policy and Procedures

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (OneOrMore): organization-level;mission/business process-level;system-level] risk assessment policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the risk assessment policy and the associated risk assessment controls;

b. Designate an [an official to manage the risk assessment policy and procedures is defined;] to manage the development, documentation, and dissemination of the risk assessment policy and procedures; and

c. Review and update the current risk assessment:

1. Policy [at least annually] and following [events that would require the current risk assessment policy to be reviewed and updated are defined;] ; and

2. Procedures [at least annually] and following [significant changes].

|  |
| --- |
| **RA-1 Control Summary Information** |
| Responsible Roles: SOP Team, Policy |
| Parameter ra-1(a): all personnel |
| Parameter ra-01\_odp.01: |
| Parameter ra-01\_odp.02: |
| Parameter ra-01\_odp.03: a Microsoft-wide |
| Parameter ra-01\_odp.04: the Microsoft Information Risk Management Council (IRMC) organization |
| Parameter ra-01\_odp.05: at least annually |
| Parameter ra-01\_odp.06: significant changes |
| Parameter ra-01\_odp.07: at least annually |
| Parameter ra-01\_odp.08: significant changes |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☒ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **RA-1 What is the solution and how is it implemented?** |
| **Part A1**  **Customer Responsibility**  The customer is responsible for developing, documenting, and disseminating risk assessment policy and procedures that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.  **Azure**  Azure addresses the risk assessment policy as part of the Microsoft security policies, of which there are two sets: the Microsoft Security Policy (MSP) that is applicable to all personnel, and the Microsoft Security Program Policy (MSPP), which is applicable to all personnel that have a responsibility for security. The Microsoft Information Risk Management Council (IRMC) is the governance body with review and approval responsibility for the MSP and MSPP. Within Azure, the MSPP specifically applies to all personnel involved in designing, building, and operating Azure and across all information and processes used in the conduct of Microsoft business. All Azure personnel are accountable and responsible for complying with these guiding principles within their designated roles. The policy addresses the following:  Azure addresses the risk assessment policy as part of the Microsoft security policies, of which there are two sets: the Microsoft Security Policy (MSP) that is applicable to all Microsoft personnel, and the Microsoft Security Program Policy (MSPP), which is applicable to all Microsoft personnel that have a responsibility for security. The Microsoft Information Risk Management Council (IRMC) is the governance body with review and approval responsibility for the MSP and MSPP. Within Azure, the MSPP specifically applies to all Microsoft personnel with security objectives such as designing, building, and operating Azure and across all information and processes used in the conduct of Microsoft business. All Azure personnel are accountable and responsible for complying with these guiding principles within their designated roles. The policy addresses the following:  \* Organizational Risk Assessment  \* Compliance Framework Management  Additionally, the policy addresses the purpose, scope, roles, responsibilities, compliance requirements, and required coordination among the various Microsoft organizations that provide some level of support to all services. The standards indicate Microsoft management’s commitment and are a component of the risk management strategy which provides Azure personnel with a current set of clear and concise information security requirements.  The MSP is available to all Microsoft personnel on the Microsoft Policy website on the Microsoft intranet, and the MSPP and Security Standards are available through the Liquid tool, also on the Microsoft intranet. The Azure SOPs are stored in the Azure Security, Privacy & Compliance SharePoint site. This SharePoint site is accessible to all Azure personnel.  Service teams may supplement the Azure policies and procedures with offering-specific policies and procedures. Service-team-specific policies and procedures associated with risk assessment are documented and stored within internal Azure SharePoint sites. Only personnel with authorized credentials, adequate levels of permission, legitimate need to know, and specific roles and responsibilities are given access to the service-team-specific policies or procedures. |
| **Part A2**  **Customer Responsibility**  The customer is responsible for procedures to facilitate the implementation of the risk assessment policy and the associated risk assessment controls.  **Azure**  The Azure Risk and Exception Management Standard Operating Procedure (SOP) implements the risk assessment policy and associated controls and documents the following procedures:  \* Risk Assessment Approach  \* Risk Assessment Methodology  \* System Categorization  \* System Threat Environment  \* Risk Assessment Results  Service teams may supplement the Azure policies and procedures with offering-specific policies and procedures. Service-team-specific policies and procedures associated with risk assessment are documented and stored within internal Azure SharePoint sites. Only personnel with authorized credentials, adequate levels of permission, legitimate need to know, and specific roles and responsibilities are given access to the service-team-specific policies or procedures. |
| **Part B**  **Customer Responsibility**  The customer is responsible for designating an official to manage the development, documentation, and dissemination of the risk assessment policy and procedures.  **Azure**  The Microsoft Information Risk Management Council (IRMC) organization is the governance body with approval responsibility for the Microsoft Security Policy (MSP) and Microsoft Security Program Policy (MSPP). The IRMC consists of representatives from security and risk management teams across Microsoft including Core Services Engineering and Operations (CSEO), Azure, and Global Security. The Customer Security and Trust: Security Engineering (CST-SE) organization manages the review and approval process and maintains the policies.  On an annual basis, the CST-SE conducts a line-by-line review of the MSP and MSPP. The Microsoft Security Policy (MSP) and Microsoft Security Program Policy (MSPP) Governance document describes each member’s role, types and frequency of review, escalation paths, approval process, and formal publishing procedures of the security policy. Throughout the year, if necessary, CST-SE may convene with the IRMC to conduct reviews after a significant review or change request. The approved policy update is published within the relevant tool on the Microsoft intranet. If service teams establish service-specific or team-specific policies, the respective service teams update the necessary policies at least annually. |
| **Part C1**  **Customer Responsibility**  The customer is responsible for reviewing and updating the current risk assessment policy on a regular basis and following organization defined events.  **Azure**  The Azure team updates the Azure SOPs at least annually through a formal review process. If needed, the Azure team updates the SOP after a significant change affecting policy execution as well. If established, service-team-specific procedures are updated by their respective teams. The individual service teams review and update their respective SOPs at least annually and when required by a significant change. |
| **Part C2**  **Customer Responsibility**  The customer is responsible for reviewing and updating the risk assessment procedures on a regular basis and following organization defined events.  **Azure**  The Azure team updates the Azure SOPs at least annually through a formal review process. If needed, the Azure team updates the SOP after a significant change affecting policy execution as well. If established, service-team-specific procedures are updated by their respective teams. The individual service teams review and update their respective SOPs at least annually and when required by a significant change. |

## RA-2 Security Categorization

a. Categorize the system and information it processes, stores, and transmits;

b. Document the security categorization results, including supporting rationale, in the security plan for the system; and

c. Verify that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.

|  |
| --- |
| **RA-2 Control Summary Information** |
| Responsible Roles: Azure Compliance |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **RA-2 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  The customer is responsible for categorizing resources and the information contained in accordance with applicable Federal Laws, Executive Orders, directives, policies, regulations, standards, and guidance. Customer agencies/departments must separately categorize their data in agreement with FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, and NIST SP 800-60 Rev. 1, Guide for Mapping Types of Information and Information Systems to Security Categories.  **Azure**  Microsoft has completed a system categorization of the Azure information and information system in accordance with Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems, and NIST Special Publication 800-60 Volume 1 Revision 1, Guide for Mapping Types of Information and Information Systems to Security Categories.  Azure completed a Security Authorization package that undergoes the process for a Provisional Authorization to Operate at a High/High/High impact level with appropriate security control overlays. Security categorization is a function of the data and the system. Azure is categorized as a FedRAMP High and DoD IL2 system. |
| **Part B**  **Customer Responsibility**  The customer is responsible for documenting the security categorization results, including supporting rationale, defined in RA-02.a in the security plan.  **Azure**  The security categorization for Azure has been conducted and is documented in section 2 of this SSP. The overall security categorization has been assessed at the High impact level for CIA respectively as determined in accordance with Federal Information Processing Standards (FIPS) 199, Committee on National Security Systems Instruction (CNSSI) Number 1253, and Intelligence Community Directive (ICD) 503 guidelines. The security categorization process took into consideration supporting rationale for impact-level decisions and involved appropriate stakeholders and senior level organizational officials to review and approve the final security categorization activity. |
| **Part C**  **Customer Responsibility**  The customer is responsible for ensuring the security categorization decision is reviewed and approved by the authorizing official (AO) or designated representative responsible.  **Azure**  Microsoft has provided the security categorization assessment in the Azure security authorization package for the review and approval of the FedRAMP JAB, DISA/DoD authorizing officials, and other regulators as required utilizing Azure. |

## RA-3 Risk Assessment

a. Conduct a risk assessment, including:

1. Identifying threats to and vulnerabilities in the system;

2. Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and

3. Determining the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information;

b. Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments;

c. Document risk assessment results in [Selection: security and privacy plans;risk assessment report;[a document in which risk assessment results are to be documented (if not documented in the security and privacy plans or risk assessment report) is defined (if selected);] ] ;

d. Review risk assessment results [at least annually and whenever a significant change occurs];

e. Disseminate risk assessment results to [personnel or roles to whom risk assessment results are to be disseminated is/are defined;] ; and

f. Update the risk assessment [annually] or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system.

Guidance: Significant change is defined in NIST Special Publication 800-37 Revision 2, Appendix F.

(e) Requirement: Include all Authorizing Officials; for JAB authorizations to include FedRAMP.

|  |
| --- |
| **RA-3 Control Summary Information** |
| Responsible Roles: Azure Compliance |
| Parameter ra-03\_odp.01: Security Assessment Report |
| Parameter ra-03\_odp.02: |
| Parameter ra-03\_odp.03: at least annually and whenever a significant change occurs |
| Parameter ra-03\_odp.04: personnel or roles with risk assessment responsibilities, as well as AOs and FedRAMP ISSOs |
| Parameter ra-03\_odp.05: annually |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **RA-3 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  The customer is responsible for conducting a risk assessment that addresses the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of customer-deployed resources and the information processed, stored, or transmitted.  The customer is responsible for reviewing the Azure Security Authorization package and performing a risk assessment for any controls deferred to the customer relating to shared touch points as identified in the Azure Customer Responsibility Matrix.  **Azure**  Microsoft conducts assessments of the risk including the likelihood and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of Azure and the information it processes, stores, or transmits. The Security Assessment for Azure was completed in agreement with NIST Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments, and NIST Special Publication 800-53A Revision 4, Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans.  Periodic risk assessments are performed for Azure to review the effectiveness of existing information security controls and safeguards, as well as to identify new risks. These assessments ensure all policies and supporting procedures properly address the environment in light of changing regulatory, contractual, business, technical, and operational requirements. Risk assessments take place annually, or more frequently as circumstances necessitate. |
| **Part B**  **Customer Responsibility**  The customer is responsible for integrating risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments for customer-deployed resources.  **Azure**  Periodic risk assessments are performed for Azure to review the effectiveness of existing information security controls and safeguards, as well as to identify new risks. These assessments ensure all policies and supporting procedures properly address the environment in light of changing regulatory, contractual, business, technical, and operational requirements. The risk assessment results are integrated with risk management decisions and remediation plans for Azure. Risk assessments take place annually, or more frequently as circumstances necessitate. |
| **Part C**  **Customer Responsibility**  The customer is responsible for conducting a risk assessment and documenting the risk assessment results in the security plan, risk assessment report, and/or other customer-defined document.  **Azure**  The Azure security risk assessment takes place during the annual assessment. The assessment is conducted in accordance with the approved Security Assessment Plan (SAP). The security assessment results are documented under Security Assessment Report (SAR) report. The security assessment is completed by an approved Third Party Assessment Organization (3PAO). |
| **Part D**  **Customer Responsibility**  The customer is responsible for conducting a risk assessment and reviewing its results at a customer-defined frequency.  **Azure**  The risk assessment is completed as part of the original security authorization package and reviewed by Microsoft annually, or when a significant change occurs as defined in NIST Special Publication 800-37 Revision 2, Guide for Applying the Risk Management Framework to Federal Information Systems, Appendix F, Page F-7. |
| **Part E**  **Customer Responsibility**  The customer is responsible for conducting a risk assessment and disseminating its results to customer-defined personnel/roles.  **Azure**  Azure submits risk assessment results to Azure management, including the Azure Program Managers. The annual SAR is submitted to the FedRAMP JAB, DISA/DoD authorizing officials, and other regulators as required who review the package for sufficiency. Internally, the SAR is used to update the POA&M submissions. |
| **Part F**  **Customer Responsibility**  The customer is responsible for updating the risk assessment at the customer-defined frequency, when there are significant changes to customer-deployed resources (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.  **Azure**  The risk assessment is completed as part of the original security authorization package and is updated by Microsoft annually, or when a significant change occurs as defined in NIST Special Publication 800-37 Revision 2, Guide for Applying the Risk Management Framework to Federal Information Systems, Appendix F, Page F-7. The information system may require an update to the risk assessment including, but not limited to, when one or more of the following circumstances occur:  \* Addition or replacement of a major component or a significant part of a major system  \* A change in security mode of operation  \* A change in interfacing systems  \* A significant change to the operating system or executive software  \* A breach of security, violation of system integrity, or any unusual situation that appears to invalidate the accreditation  \* A significant change to the physical structure housing the information system or environment of the information system that could affect the physical security described in the accreditation  \* A significant change to the threat that could adversely affect the systems  \* A significant change to the availability of safeguards  \* A significant change to the user population  If any of these events should occur, the SSP and other affected Security Authorization Process documentation are updated to reflect the new information system components, or new operating environment. Changes are coordinated with the Azure authorizing officials and an updated package submitted for review and consideration. |

### RA-3(1) - Supply Chain Risk Assessment

(a) Assess supply chain risks associated with [systems, system components, and system services to assess supply chain risks are defined;] ; and

(b) Update the supply chain risk assessment [the frequency at which to update the supply chain risk assessment is defined;] , when there are significant changes to the relevant supply chain, or when changes to the system, environments of operation, or other conditions may necessitate a change in the supply chain.

|  |
| --- |
| **RA-3(1) Control Summary Information** |
| Responsible Roles: Supply Chain |
| Parameter ra-03.01\_odp.01: Azure system components |
| Parameter ra-03.01\_odp.02: annually |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **RA-3(1) What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  The customer is responsible for assessing supply chain risks associated with customer-defined and controlled systems, system components, and system services.  **Azure**  "One Microsoft" Supply Chain assurance efforts consist of numerous capabilities executing a corporate strategy that contributes to protecting Azure. The following efforts take place for Azure to assess and review the supply chain-related risks associated with Azure cloud components on an at least annual cadence.  **Procurement**  During the initial supply chain phase, the Procurement team protects against supply chain threats by facilitating the creation of the purchase order to our suppliers ensuring consistency in approach.  <https://www.microsoft.com/en-us/procurement/supplier-contracting.aspx>  **Customer Operations**  Customer Operations performs routine business reviews with our suppliers representing the needs and concerns of all Azure business groups. This team also works to support Azure business groups on standards definition and service capability. A key function of this team is to protect against any threats posed by suppliers during manufacturing by ensuring adherence to standard supply chain methodologies and process adherence.  **Deployment Quality**  System integration or upon delivery of services to our Azure datacenters for deployment; Deployment Quality works to ensure final delivery of the system to the Azure business group is done on-time and free of defects. Working in conjunction with the Supply Chain Automation, these capabilities monitor performance metrics, capture business group feedback, and lead cross-functional Supply Chain.  **Supplier Relationship Management (SRM)**  As services move into the operations and maintenance phase of the life cycle, SRM protects Azure by managing and facilitating the supplier complaint process to drive root cause and corrective action within the suppliers’ supply chain. Supplier scorecards allow Azure to compare and visibly monitor the performance of our supply base utilizing a balanced scorecard approach.  **Spares**  Spares Management protects against supply chain threats by managing the determination and execution of obtaining spare components to support deployed devices within our Azure datacenters. Parts are spared to significantly reduce downtime of production equipment during a trouble-shooting scenario, helping to ensure site uptime for our business.  To ensure security of the supply chain and protection against threats, Azure uses well-established suppliers with a proven track record to secure supply chain management. In addition, these suppliers have established Service Level Agreements with critical providers to ensure that additional spare parts and maintenance activities are performed in a timely manner.  **Business Continuity**  Microsoft manages a comprehensive Continuity of Supply program with redundancies across Systems Integrators and components suppliers wherever possible. There is a team which drives continuous analysis of multi-source vs single source and end of life transitions for components across the Bill of Materials. Strategic purchases and inventories are held in an ongoing program to ensure supply of critical components and last time purchases. Supplier financial health is assessed routinely with risk assessments and deeper engagements on areas of concern.  **Asset Classification and Risk**  Assessments are determined by a "One Microsoft" team at initial infrastructure design and build to meet market/customer compliance boundary requirements. In addition, there are existing process for each service to provide its offering in each boundary. In addition, processes are in place for designated high integrity devices and services.  **Logistics**  Microsoft continues to increase assurance in the complex cloud global supply chain with next generation visibility by implementing a new global control tower capability, the next generation of supply chain visibility. The new capability delivers proactive intelligence on potential disruptions including weather, traffic, and global events, that allows Microsoft to notify our customer as the disruptions occur to adjust and deliver successfully. In addition, Microsoft is placing sensors on high value shipments with GPS capability supported by light and temperature detections at fifteen (15) minute tracking intervals.  **Validation**  Microsoft employs a capability to discover, configure, and validate in-rack hardware. The validation is executed at the original equipment manufacturer (OEM) prior to shipment and again at the Microsoft datacenter.  **Firmware**  Microsoft employs firmware source code guidance, reviews, and penetration tests to identify security vulnerabilities at the firmware level.  **Global Security Ecosystem Support**  Capabilities including Threat Intelligence, Digital Crime Unit, Cyber Defense Operations Center, and Service Security Teams, the Azure Red Team coordinated overt and covert activities to validate and strengthen the Global Azure and Specific Sovereign Infrastructures. In addition, the Third Party Assessment Organization (3PAO) penetration tests are part of the overall certifications.  **Industry Leadership**  The Microsoft Supply Chain Security program maintains industry-leading low loss levels across the various supply chains for the past five (5) years. Microsoft is Tier 3 certified with Customs Trade Partnership Against Terrorism (CTPAT), a Homeland Security / Customs and Border Protection program, and Authorized Economic Operator (AEO) certified in India, pending Australia.  **Global Leadership and Partnerships**  Microsoft members maintain leadership roles in the Transported Asset Protection Association (TAPA) and the Alliance for Gray Market and Counterfeit Abatement (AGMA). In addition, Microsoft maintains active representation in the European Union, North Atlantic Treaty Organization, and World Trade Organization. |
| **Part B**  **Customer Responsibility**  The customer is responsible for updating the supply chain risk assessment at a customer-defined frequency when there are significant changes to relevant supply chain, or when changes to the system, environments of operation, or other conditions may necessitate a change in the supply chain for customer-deployed resources.  **Azure**  Azure updates supply chain risk assessments conducted for Azure cloud components at least on an annual basis or whenever changes to the relevant supply chain, or when changes to Azure cloud components, environments of operation, or other conditions may necessitate a change in the supply chain. The supply chain risk assessments are documented and retained for investigation purposes. |

## RA-5 Vulnerability Monitoring and Scanning

a. Monitor and scan for vulnerabilities in the system and hosted applications [monthly operating system/infrastructure; monthly web applications (including APIs) and databases] and when new vulnerabilities potentially affecting the system are identified and reported;

b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:

1. Enumerating platforms, software flaws, and improper configurations;

2. Formatting checklists and test procedures; and

3. Measuring vulnerability impact;

c. Analyze vulnerability scan reports and results from vulnerability monitoring;

d. Remediate legitimate vulnerabilities [high-risk vulnerabilities mitigated within thirty (30) days from date of discovery; moderate-risk vulnerabilities mitigated within ninety (90) days from date of discovery; low risk vulnerabilities mitigated within one hundred and eighty (180) days from date of discovery] in accordance with an organizational assessment of risk;

e. Share information obtained from the vulnerability monitoring process and control assessments with [personnel or roles with whom information obtained from the vulnerability scanning process and control assessments is to be shared;] to help eliminate similar vulnerabilities in other systems; and

f. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.

Guidance: See the FedRAMP Documents page> Vulnerability Scanning Requirements https://www.FedRAMP.gov/documents/

(a) Requirement: an accredited independent assessor scans operating systems/infrastructure, web applications, and databases once annually.

(d) Requirement: If a vulnerability is listed among the CISA Known Exploited Vulnerability (KEV) Catalog (https://www.cisa.gov/known-exploited-vulnerabilities-catalog) the KEV remediation date supersedes the FedRAMP parameter requirement.

(e) Requirement: to include all Authorizing Officials; for JAB authorizations to include FedRAMP

Guidance: Informational findings from a scanner are detailed as a returned result that holds no vulnerability risk or severity and for FedRAMP does not require an entry onto the POA&M or entry onto the RET during any assessment phase. Warning findings, on the other hand, are given a risk rating (low, moderate, high or critical) by the scanning solution and should be treated like any other finding with a risk or severity rating for tracking purposes onto either the POA&M or RET depending on when the findings originated (during assessments or during monthly continuous monitoring). If a warning is received during scanning, but further validation turns up no actual issue then this item should be categorized as a false positive. If this situation presents itself during an assessment phase (initial assessment, annual assessment or any SCR), follow guidance on how to report false positives in the Security Assessment Report (SAR). If this situation happens during monthly continuous monitoring, a deviation request will need to be submitted per the FedRAMP Vulnerability Deviation Request Form. Warnings are commonly associated with scanning solutions that also perform compliance scans, and if the scanner reports a "warning" as part of the compliance scanning of a CSO, follow guidance surrounding the tracking of compliance findings during either the assessment phases (initial assessment, annual assessment or any SCR) or monthly continuous monitoring as it applies. Guidance on compliance scan findings can be found by searching on "Tracking of Compliance Scans" in FAQs.

|  |
| --- |
| **RA-5 Control Summary Information** |
| Responsible Roles: Scanning |
| Parameter ra-5(a): monthly operating system/infrastructure; monthly web applications (including APIs) and databases |
| Parameter ra-05\_odp.01: |
| Parameter ra-05\_odp.02: |
| Parameter ra-05\_odp.03: high-risk vulnerabilities mitigated within thirty (30) days from date of discovery; moderate-risk vulnerabilities mitigated within ninety (90) days from date of discovery; low risk vulnerabilities mitigated within one hundred and eighty (180) days from date of discovery |
| Parameter ra-05\_odp.04: Azure Security, Azure Compliance, FedRAMP |
| Implementation Status (check all that apply):  ☐ Implemented  ☒ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **RA-5 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for performing periodic vulnerability scanning on all customer-deployed resources, including applications built on those resources. Customers are responsible for performing scans of their applications running within or connected to their purchased Azure VMs or deployments. Detailed information regarding customer implementations of threat mitigating security practices can be accessed through the external Azure Trust Center.  **Azure**  Azure implements vulnerability scanning by actively scanning virtual (PaaS and IaaS) and physical servers, network devices, databases, and web applications in the Azure inventory with authenticated scans. Scans are performed monthly, daily or multiple times per day depending on the asset type. The vulnerability scanning tools provide Azure updates as new vulnerabilities are identified and reported.  Scans are also performed when newly identified vulnerabilities are added for each type of scan. The C+AI VSA team within Azure manages the vulnerability management program and provides scanning services for the environment. C+AI VSA is responsible for the identification, assessment, and notification of vulnerabilities to Azure personnel, who are responsible for the remediation of verified vulnerabilities on operating systems, 1st and 3rd party software, network elements and applications deployed in the Azure environment.  Listed below are the assets scanned each month in accordance with the monthly assignment:  \* Twice a day operating system (OS) and 1st and 3rd-party software scans are performed for  \* PaaS, IaaS VMs, Native, and Pilotfish server environments  \* Physical (bare metal) server environment  \* Monthly operating system (OS) Scans are performed for  \* Azure network devices  \* Monthly database (DB) scans are performed for  \* SQL DB instances  \* Monthly web application scans are performed for  \* Web applications (hosted URLs)  In addition, the Third Party Assessment Organization (3PAO) satisfies the requirements for independent third-party security assessment and scanning on an annual basis. This is done by having the Third Party Assessment Organization (3PAO) review the scanning configuration, observe the scan where possible, and review the results.  A TLS scanner hosted by Unified Remoting Scanning (URSA) is used to determine the status of Azure encryption in transit, specifically the use of TLS 1.2/1.3 or higher. |
| **Part B**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for employing vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process.  **Azure**  Azure employs automated vulnerability scanning tools to scan the Azure operating systems, 1st and 3rd party software, databases, and web applications. The vulnerability scanning tools provide reporting data based on a number of existing, well-used, open standards that itemize software flaws, security configurations, and various product names, including the Common Vulnerabilities and Exposures (CVE) and Common Vulnerability Scoring System (CVSS). The following sections address the scanning tools and techniques used for each applicable Azure asset type.  Azure utilizes a variety of well-known knowledge-based scan tools with the applicable plugins to run authenticated vulnerability scans on a predetermined number of servers depending on the asset type. Scan tool plugins are updated prior to scanning any hosts. Azure employs the following predetermined scanning methodologies to perform authenticated scans:  **Physical Servers**  >98% of Azure physical server operating systems with AzSecpack installed are scanned with credentials using the Qualys-based off-node vulnerability scanner including virtual (Azure SQL) database and web application hosts. All scans are authenticated.  **Physical Database Instances**  100% of all physical databases are scanned with credentials the VA Scan Tool.  **Virtual Servers**  Authenticated scans are performed on >95% of Azure service team servers. Azure scans virtual servers using the Microsoft-specific Qualys-based off-node vulnerability scanner.  **Virtual Database Instances**  >98% of Azure virtual database instances where AzSecpack is installed are scanned for vulnerabilities and for database compliance checks.  **Web Applications**  Microsoft SDL requires that service team site owners onboard their externally facing sites for security scanning. This requires service team site owners to create scanning profiles which includes providing authentication information (if it exists) and to ensure scans run monthly. The Unified Remote Scanning Architecture (URSA) ensures that 100% onboarded sites are scanned at the services set schedule and any issues found are reported. Web Application scanning is using Rapid7 AppSpider with applicable web application plug-ins enabled which is referred to internally as WebScanner (a component of URSA).  **Network Devices**  85% of Azure network devices are scanned with authenticated scans using Qualys. |
| **Part C**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for analyzing scan reports and results from vulnerability monitoring.  **Azure**  The Vulnerability Management team assesses the vulnerability severity and impact level based on documented technology deployed and used in the Azure environment.  C+AI VSA collects information from a variety of vulnerability scanning tools to help determine the inventory of applications installed on servers to assess the current threat surface. Configuration checks are performed against the C+AI VSA managed Azure baselines. The C+AI Security team reviews configurations as part of the vulnerability scanning tool reports and performs a risk analysis in determining scores for impact and likelihood. Specific steps in the vulnerability process include:  \* Review mitigating controls that may affect the vulnerability rating such as implementation of firewalls, antivirus and anti-malware software, access control lists (ACLs), and more.  \* Review the Asset Value for the affected assets.  \* Determine the timeframe for the application of the required updates. |
| **Part D**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for remediating vulnerabilities in customer-deployed resources in accordance with the customer risk assessment.  **Azure**  Vulnerabilities are classified by risk and applicability to the environment with all vulnerabilities identified by C+AI VSA required to be remediated within thirty (30) days for high, ninety (90) days for moderate, and one hundred and eighty (180) days for low risk vulnerabilities. In addition, all verified security flaws are managed and tracked via the POA&M process. |
| **Part E**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for sharing information obtained from the vulnerability scanning process and security control assessments to help eliminate similar vulnerabilities across customer-deployed resources.  **Azure**  The C+AI Vulnerability Management team regularly communicates relevant information obtained during the scanning process with the appropriate Microsoft Online Services personnel to eliminate duplicate efforts and to facilitate the remediation process. Reporting of security vulnerabilities is conducted via the vulnerability management and reporting tool, S360 and focused e-mails. The vulnerability management and reporting tools provide reports based on multiple criteria, including property, server and security flaws identified from the vulnerability scans and is accessible by Azure personnel at any time. E-mail communication from the Vulnerability Management team is used to notify asset owners in cases of elevated risk or when expedited action is necessary.  In addition, Azure shares information obtained from the vulnerability scanning process and security control assessments with the ISSO/ISSM monthly via the Continuous Monitoring Reports and POA&M. |
| **Part F**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for employing the capability to update vulnerability scanning tools.  **Azure**  The vulnerability scanning tools used within the Azure environment include the capability to readily update the list of information system vulnerabilities to be scanned. The tools release new vulnerability definitions as needed following the publication of Common Vulnerability and Exposures (CVE) information. New signature files are updated either before each scan or, for Qualys off-node scan signatures, at least weekly, with scans performed daily. |

### RA-5(2) - Update Vulnerabilities to Be Scanned

Update the system vulnerabilities to be scanned [Selection (OneOrMore): [the frequency for updating the system vulnerabilities to be scanned is defined (if selected);] ;prior to a new scan;when new vulnerabilities are identified and reported] .

|  |
| --- |
| **RA-5(2) Control Summary Information** |
| Responsible Roles: Scanning |
| Parameter ra-05.02\_odp.01: prior to a new scan |
| Parameter ra-05.02\_odp.02: |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **RA-5(2) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for updating the list of vulnerabilities scanned prior to a new scan, when new vulnerabilities are identified and reported, and/or at the customer-defined frequency.  **Azure**  The vulnerability scanning tools used within the Azure environment include the capability to readily update the list of information system vulnerabilities to be scanned. The tools release new vulnerability definitions as needed following the publication of Common Vulnerability and Exposures (CVE) information. New signature files are updated either before each scan or, for Qualys off-node scan signatures, at least weekly, with scans performed daily. |

### RA-5(3) - Breadth and Depth of Coverage

Define the breadth and depth of vulnerability scanning coverage.

|  |
| --- |
| **RA-5(3) Control Summary Information** |
| Responsible Roles: Scanning |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **RA-5(3) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for employing vulnerability scanning procedures that identify the breadth and depth of scanning coverage.  **Azure**  To meet the appropriate breadth and depth of coverage, Azure utilizes vulnerability scanning tools to conduct authenticated scans of all asset types within the Azure security authorization boundary. Vulnerability scans of the Azure web applications and databases are conducted using vulnerability scanning tools with applicable web application and database plug-ins enabled. All scanning results are based on the latest plugins available to ensure all areas are covered in appropriate depth. In addition, for database instance scanning, appropriate tools are used to ensure database compliance checks are enabled. |

### RA-5(4) - Discoverable Information

Determine information about the system that is discoverable and take [notify appropriate service provider personnel and follow procedures for organization and service provider-defined corrective actions].

|  |
| --- |
| **RA-5(4) Control Summary Information** |
| Responsible Roles: Publicly Accessible Content |
| Parameter ra-05.04\_odp: notify appropriate service provider personnel and follow procedures for organization and service provider-defined corrective actions |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **RA-5(4) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for taking action in response to customer information that is discoverable by adversaries.  **Azure**  Microsoft’s Marketing Communications team conducts weekly scans on social media engines such as X and LinkedIn using keywords like Microsoft, Microsoft Datacenter, competitor names, product names, and more to identify any disclosed nonpublic information. Additionally, all publicly available white papers are updated and reviewed by the Marketing Communications team on a quarterly basis.  If any nonpublic information is identified as part of reviews, the Azure incident management process is followed to investigated and remediate the issue. |

### RA-5(5) - Privileged Access

Implement privileged access authorization to [all components that support authentication] for [all scans].

|  |
| --- |
| **RA-5(5) Control Summary Information** |
| Responsible Roles: Scanning |
| Parameter ra-05.05\_odp.01: all components that support authentication |
| Parameter ra-05.05\_odp.02: all scans |
| Implementation Status (check all that apply):  ☐ Implemented  ☒ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **RA-5(5) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for implementing privileged access for executing customer-defined vulnerability scanning activities.  **Azure**  Azure includes elevated access authorization to operating systems, databases, and web applications for authenticated vulnerability scanning to facilitate more thorough scanning. Azure utilizes vulnerability scanning tools to conduct authenticated scans of the devices within the Azure security authorization boundary. Vulnerability scans are conducted using vulnerability scanning tools with applicable web application and database plug-ins enabled or specialized tools where appropriate. |

### RA-5(8) - Review Historic Audit Logs

Review historic audit logs to determine if a vulnerability identified in a [a system whose historic audit logs are to be reviewed is defined;] has been previously exploited within an [a time period for a potential previous exploit of a system is defined;].

Requirement: This enhancement is required for all high (or critical) vulnerability scan findings.

|  |
| --- |
| **RA-5(8) Control Summary Information** |
| Responsible Roles: Incident Response, Scanning |
| Parameter ra-05.08\_odp.01: operating systems, databases, and web applications in the Azure environment |
| Parameter ra-05.08\_odp.02: as needed |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **RA-5(8) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for reviewing historic audit logs to determine if a vulnerability identified within customer-deployed resources has been previously exploited.  **Azure**  Azure implements audit review, analysis, and reporting through the use of Azure logging and monitoring tools for both server baselines and network devices. The automated tooling processes logs for anomalous activity and sends alerts and incident tickets as needed.  Additionally, to identify vulnerabilities, Azure conducts scans of operating systems, databases, and web applications in the Azure environment. Multiple sources of information for vulnerability-related data are used for these scans including MSRC, vendor websites, and other third-party websites. The Security Response Team reviews historic log data as needed for incident investigation. |

### RA-5(11) - Public Disclosure Program

Establish a public reporting channel for receiving reports of vulnerabilities in organizational systems and system components.

|  |
| --- |
| **RA-5(11) Control Summary Information** |
| Responsible Roles: Incident Response, Continuous Monitoring, Scanning |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **RA-5(11) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for establishing a public reporting channel for receiving reports of vulnerabilities in organizational systems and system components for customer-deployed resources.  **Azure**  The Azure Continuous Monitoring and Azure Security teams establish public reporting channels for receiving reports of vulnerabilities. The Azure Security Team has websites external customers can leverage to report vulnerabilities. The Azure Continuous Monitoring team members have subscriptions from external websites that report vulnerabilities such as from Cybersecurity Infrastructure Security Agency (CISA), Qualys KB, Qualys vulnerability scanning, MSRC internal Microsoft communications, NIST, and NVD websites. Vulnerabilities obtained from external channels are assessed to determine if they impact Azure compliance boundary. If found to impact Azure compliance boundary, the Azure Continuous Monitoring team tracks the vulnerabilities as open POA&Ms and coordinate with Azure Security and Service Teams to dive the vulnerabilities to closure. |

## RA-7 Risk Response

Respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance.

|  |
| --- |
| **RA-7 Control Summary Information** |
| Responsible Roles: Azure Compliance, Continuous Monitoring |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **RA-7 What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for responding to findings from security and privacy assessments, monitoring, and audits in accordance with customer risk tolerance for customer-deployed resources.  **Azure**  Azure employs an approved Third-Party Assessment Organization (3PAO) as an independent assessor to conduct a security control assessment of Azure in accordance with security control requirements. Azure adds findings identified in 3PAO monthly continuous monitoring and annual audit assessments into Plan of Actions & Milestone (POA&M) spreadsheets for remediation tracking. Depending on the risk of the finding, Azure takes appropriate action to remediate findings in accordance with FedRAMP Continuous Monitoring Guidelines. The results of this assessment and related activities are submitted to Azure’s authorizing officials. |

## RA-9 Criticality Analysis

Identify critical system components and functions by performing a criticality analysis for [systems, system components, or system services to be analyzed for criticality are defined;] at [decision points in the system development life cycle when a criticality analysis is to be performed are defined;].

|  |
| --- |
| **RA-9 Control Summary Information** |
| Responsible Roles: Azure Compliance, SDL, Asset Management, Datacenter Hosting, Supply Chain |
| Parameter ra-09\_odp.01: all information system services |
| Parameter ra-09\_odp.02: Privacy Manager completion |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **RA-9 What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for identifying critical information system components and functions by performing a criticality analysis for customer-defined information systems, information system components, or information system services at customer-defined decision points in the system development life cycle.  **Azure**  To identify and apply the appropriate asset classification, the Microsoft Asset Owner performs the following steps:  \* Business Requirements: The Asset Owner identifies any unique requirements that apply to the Online Service based on use-case scenarios and business requirements. This includes understanding data requirements as described in the Data Classification Standard.  \* Risk Evaluation: The Asset Owner assesses the risks and the impacts that would be related to the asset if its confidentiality, integrity, or availability were to be compromised. Impact criteria are defined in the Asset Classification Standard.  \* Classification: The Asset Owner selects the appropriate classification based on the risk and valuation of the asset.  \* Protection: The Asset Owner directs the application of security protection measures and controls required by the asset classification (per the Asset Protection Standard) as well as any additional required controls.  \* Periodic Monitoring: The Asset Owner periodically reviews the risks and classification of the asset to ensure they remain appropriate or corrects them as needed.  The criteria describe the impact that would be incurred by Microsoft, Microsoft’s shareholders, partners, or customers, the Asset Owner's organization, or dependent or reliant organizations if the asset’s confidentiality, integrity, or availability were to be compromised. In some scenarios multiple types of impact may apply; the Asset Owner then chooses the highest and/or most relevant impact when making the classification decision. |

# System and Services Acquisition (SA)

## SA-1 Policy and Procedures

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (OneOrMore): organization-level;mission/business process-level;system-level] system and services acquisition policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the system and services acquisition policy and the associated system and services acquisition controls;

b. Designate an [an official to manage the system and services acquisition policy and procedures is defined;] to manage the development, documentation, and dissemination of the system and services acquisition policy and procedures; and

c. Review and update the current system and services acquisition:

1. Policy [at least annually] and following [events that would require the current system and services acquisition policy to be reviewed and updated are defined;] ; and

2. Procedures [at least annually] and following [significant changes].

|  |
| --- |
| **SA-1 Control Summary Information** |
| Responsible Roles: SOP Team, Policy |
| Parameter sa-1(a): all personnel |
| Parameter sa-01\_odp.01: |
| Parameter sa-01\_odp.02: |
| Parameter sa-01\_odp.03: a Microsoft-wide |
| Parameter sa-01\_odp.04: the Microsoft Information Risk Management Council (IRMC) organization |
| Parameter sa-01\_odp.05: at least annually |
| Parameter sa-01\_odp.06: significant changes |
| Parameter sa-01\_odp.07: at least annually |
| Parameter sa-01\_odp.08: significant changes |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☒ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SA-1 What is the solution and how is it implemented?** |
| **Part A1**  **Customer Responsibility**  The customer is responsible for developing, documenting, and disseminating system and services acquisition policy and procedures that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.  **Azure**  Azure addresses the system and services acquisition policy as part of the Microsoft security policies, of which there are two sets: the Microsoft Security Policy (MSP) that is applicable to all Microsoft personnel, and the Microsoft Security Program Policy (MSPP), which is applicable to all Microsoft personnel that have a responsibility for security. The Microsoft Information Risk Management Council (IRMC) is the governance body with review and approval responsibility for the MSP and MSPP. Within Azure, the MSPP specifically applies to all Microsoft personnel with security objectives such as designing, building, and operating Azure and across all information and processes used in the conduct of Microsoft business. All Azure personnel are accountable and responsible for complying with these guiding principles within their designated roles. The policy addresses the following:  \* Ownership of third-party relationships  \* Security Development Lifecycle (SDL)  \* Introduction of new hardware, software, or services  Additionally, the policy addresses the purpose, scope, roles, responsibilities, compliance requirements, and required coordination among the various Microsoft organizations that provide some level of support to all services. The policies indicate Microsoft management’s commitment and are a component of the risk management strategy which provides Azure personnel with a current set of clear and concise information security requirements.  The MSP is available to all Microsoft personnel on the Microsoft Policy website on the Microsoft intranet, and the MSPP and Security Standards are available through the Liquid tool, also on the Microsoft intranet. The Azure SOPs are stored in the Azure Security, Privacy & Compliance SharePoint site. This SharePoint site is accessible to all Azure personnel.  Service teams may supplement the Azure policies and procedures with offering-specific policies and procedures. Service-team-specific policies and procedures associated with system and services acquisition are documented and stored within internal Azure SharePoint sites. Only personnel with authorized credentials, adequate levels of permission, legitimate need to know, and specific roles and responsibilities are given access to the service-team-specific policies or procedures. |
| **Part A2**  **Customer Responsibility**  The customer is responsible for procedures to facilitate the implementation of system and services acquisition policy and the associated system and services acquisition controls.  **Azure**  To meet controls for system and services acquisition, Azure maintains teams with responsibilities to procure professional services, review contracts to Microsoft corporate standards, and procure assets for the delivery of Azure services. Multiple standards, processes, and SOPs are maintained by individual Azure teams to support the implementation and adherence to the MSPP section on Supplier Relationships.  Microsoft system and services procurement activities are managed through a company-wide team. All external suppliers of services or systems must be approved by the Global Procurement Group (GPG) and have a signed contract and Master Supplier Services Agreement (MSSA) on file. The contract includes sections outlining security requirements and service level monitoring to be enforced. GPG requires the external suppliers of services to comply with all applicable Microsoft security policies and implement security procedures to prevent disclosure of Microsoft Confidential information. Microsoft includes provisions in the MSSA and any associated Statements of Work (SOW) with each vendor addressing the need to employ appropriate security controls. Additionally, vendors that handle high business impact data must be in annual compliance with the Microsoft Supplier Security and Privacy Assurance (SSPA) Program Guide.  Statements of Work (SOW) and Purchase Orders (PO) can only be submitted for suppliers who have approved contracts. The GPG team as well as Microsoft’s Corporate, External, and Legal Affairs (CELA) review these documents before being approved.  These materials are formally documented and stored within each team’s internal Azure SharePoint site as a central repository. Only individuals with authorized credentials, adequate levels of permission, legitimate need to know, and specific roles/responsibilities are given access to the material. |
| **Part B**  **Customer Responsibility**  The customer is responsible for designating an official to manage the development, documentation, and dissemination of the system and services acquisition policy and procedures.  **Azure**  The Microsoft Information Risk Management Council (IRMC) organization is the governance body with approval responsibility for the Microsoft Security Policy (MSP) and Microsoft Security Program Policy (MSPP). The IRMC consists of representatives from security and risk management teams across Microsoft including Core Services Engineering and Operations (CSEO), Azure, and Global Security. The Customer Security and Trust: Security Engineering (CST-SE) organization manages the review and approval process and maintains the policies.  On an annual basis, the CST-SE conducts a line-by-line review of the MSP and MSPP. The Microsoft Security Policy (MSP) and Microsoft Security Program Policy (MSPP) Governance document describes each member’s role, types and frequency of review, escalation paths, approval process, and formal publishing procedures of the security policy. Throughout the year, if necessary, CST-SE may convene with the IRMC to conduct reviews after a significant review or change request. The approved policy update is published within the relevant tool on the Microsoft intranet. If service teams establish service-specific or team-specific policies, the respective service teams update the necessary policies at least annually. |
| **Part C1**  **Customer Responsibility**  The customer is responsible for reviewing and updating the current system and services acquisition policy on a regular basis and following organization defined events.  **Azure**  The Azure team updates the Azure SOPs at least annually through a formal review process. If needed, the Azure team updates the SOP after a significant change affecting policy execution as well. If established, service-team-specific procedures are updated by their respective teams. The individual service teams review and update their respective SOPs at least annually and when required by a significant change. |
| **Part C2**  **Customer Responsibility**  The customer is responsible for reviewing and updating the system and services acquisition procedures on a regular basis and following organization defined events.  **Azure**  The Azure team updates the Azure SOPs at least annually through a formal review process. If needed, the Azure team updates the SOP after a significant change affecting policy execution as well. If established, service-team-specific procedures are updated by their respective teams. The individual service teams review and update their respective SOPs at least annually and when required by a significant change. |

## SA-2 Allocation of Resources

a. Determine the high-level information security and privacy requirements for the system or system service in mission and business process planning;

b. Determine, document, and allocate the resources required to protect the system or system service as part of the organizational capital planning and investment control process; and

c. Establish a discrete line item for information security and privacy in organizational programming and budgeting documentation.

|  |
| --- |
| **SA-2 Control Summary Information** |
| Responsible Roles: SDL |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SA-2 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for determining the high-level information security and privacy requirements of customer-deployed resources in mission and business process planning.  **Azure**  Microsoft implements the allocation of resources control as part of Phase One: Requirements, of the Microsoft Security Development Lifecycle (SDL) Process.  The Requirements phase of the SDL includes considerations for security and privacy at a foundational level—and a cost analysis—when a determination is made if development and support costs for improving security and privacy are consistent with business needs. Microsoft includes a determination of security requirements at the onset of a project to allow for development teams to identify key milestones and deliverables, and permits the integration of security and privacy in a way that minimizes any disruption to plans and schedules. Security and privacy requirements analysis is performed at project inception and includes specification of minimum security requirements for the application as it is designed to run in its planned operational environment and specification and deployment of a security vulnerability/work item tracking system.  Likewise, Microsoft included information security requirements for Azure in mission/business process planning consistent with the terms of the Azure offering. |
| **Part B**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for determining, documenting, and allocating the resources required to protect customer-deployed resources as part of capital planning and investment control.  **Azure**  Microsoft annually budgets funding necessary to support all services and the corporate security and privacy posture across the entire company. Microsoft has determined, documented, and allocated the resources required to protect the information system as part of its capital budgeting process. The information security control requirements are documented in this SSP.  In addition, as part of the budgeting process, C+AI Security conducts capacity planning which includes the determination of the overall size, performance and resilience of the system. These elements are important to the overall security functionality of the system in terms of how security controls impact Azure’s performance, as well as, how the resiliency of the system supports data availability and continuity objectives. Capacity planning depends largely upon the proposed usage of the system. Processing and storage requirements for Azure are defined before development in order to ensure adequate resources are available. Azure capacity planning includes operating requirements, projected trends, new business requirements, and resistance to denial-of-service attacks in order to avoid preventable system deficiencies. The capacity planning process is through C+AI Security and part of the budget allocation. |
| **Part C**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible including a discrete line item for information security in programming and budgeting documentation when allocating resources.  **Azure**  The Microsoft Security Program Policy (MSPP) outlines the capacity planning process, to ensure adequate allocation of resources; it also includes technical requirements along with future capacity and security projections. Microsoft establishes discrete line items for information security, change management, and budgeting documentation, where required. Budgets are created for different departments within Microsoft and information security is considered. |

## SA-3 System Development Life Cycle

a. Acquire, develop, and manage the system using [system development life cycle is defined;] that incorporates information security and privacy considerations;

b. Define and document information security and privacy roles and responsibilities throughout the system development life cycle;

c. Identify individuals having information security and privacy roles and responsibilities; and

d. Integrate the organizational information security and privacy risk management process into system development life cycle activities.

|  |
| --- |
| **SA-3 Control Summary Information** |
| Responsible Roles: SDL |
| Parameter sa-3(a): Microsoft's Security Development Lifecycle (SDL) |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SA-3 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for acquiring, developing, and managing customer-deployed resources using a system development life cycle (SDLC), that incorporates information security and privacy considerations.  **Azure**  Microsoft implements lifecycle support for Azure services through its Security Development Lifecycle (SDL) process. The SDL consists of a security requirements analysis and applicability that must be completed for all service development projects. This analysis acts as a framework and includes the identification of possible risks to the finished service as well as mitigation strategies which can be implemented and tested during the development phases. A Threat Modeling security review is included during the SDL process. Microsoft integrates essential information technology (IT) security considerations defined in NIST Special Publication 800-160 Volume 1 as revised into the established Microsoft SDL process.  **Pre-SDL Requirements: Security Training**  All members of service development teams receive appropriate training to stay informed about security basics and recent trends in security and privacy. Individuals who develop services are required to attend at least one security training class each year. Security training can help ensure services are created with security and privacy in mind and can also help development teams stay current on security issues. Project team members are strongly encouraged to seek additional security and privacy education that is appropriate to their needs or products.  **SDL Core Phases**  The Microsoft SDL process includes the following phases:  \* Phase 1: Requirements - The Requirements phase of the SDL includes the project inception—when the organization considers security and privacy at a foundational level—and a cost analysis—when determining if development and support costs for improving security and privacy are consistent with business needs. This phase also includes defining security roles and responsibilities and identifying individuals with these roles and responsibilities.  \* Phase 2: Design - The Design phase is when the organization builds the plan for how to take the project through the rest of the SDL process—from implementation, to verification, to release. During the Design phase the organization establishes best practices to follow for this phase by way of functional and design specifications, and by performing risk analysis to identify threats and vulnerabilities in the service. TMA (Threat Model Analysis) is required to define all attack surfaces and their associated risks; all security gaps and risks and documented and analyzed. This security impact analysis results in dataflow documentation in order to identify all intended paths for information and potential attack vectors.  \* Phase 3: Implementation - The Implementation phase is when the organization creates the documentation and tools the customer uses to make informed decisions about how to deploy the service securely. To this end, the Implementation phase is when the organization establishes development best practices to detect and remove security and privacy issues early in the development cycle. Microsoft understands, observes, and implements the security requirements and considerations as outlined in GSA IT Security Procedural Guide 09-48, Security Language for IT Acquisition Efforts, dated September 2009 for the information system consistent with the Azure offering’s requirements.  \* Phase 4: Verification - During the Verification phase, the organization ensures that the code meets the security and privacy tenets established in the previous phases. This is done through security and privacy testing, and a security push—which is a team-wide focus on threat model updates, code review, testing, and thorough documentation review and edit. A public release privacy review is also completed during the Verification phase.  \* Phase 5: Release - The Release phase is when the organization prepares the service for consumption and prepares for what happens once the service is released. One of the core concepts in the Release phase is response planning—mapping out a plan of action, should any security or privacy vulnerabilities be discovered in the release—and this carries over to post-release, as well, in terms of response execution.  **Post-SDL Requirement: Security Servicing and Response Execution**  After a service is released, the product development team must be available to respond to any possible security vulnerabilities or privacy issues that warrant a response. In addition, the development team is required to follow the Azure Incident Management Standard Operating Procedure (SOP) for potential post-release issues.  Azure has implemented information validation through checking of data inputs as part of the SDL process. Thorough code reviews and testing are completed during the Verification Phase of the SDL prior to service being put into a production environment. The code reviews and testing check for cases of SQL injection, format string vulnerabilities, XSS, integer arithmetic, command injection, and buffer overflow vulnerabilities.  For more details on the SDL process, please refer to <https://www.microsoft.com/en-us/securityengineering/sdl.> |
| **Part B**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for managing customer-deployed resources using a system development life cycle (SDLC), which identifies and documents information security and privacy roles and responsibilities.  **Azure**  The SDL includes general criteria and job descriptions for security and privacy roles. These roles are filled during the Requirements Phase of the SDL process. These roles are consultative in nature, and provide the organizational structure necessary to identify, catalog, and mitigate security and privacy issues present in a service development project.  As part of the SDL, Azure has defined a dedicated security team responsible for conducting reviews, setting standards, and monitoring compliance with regulatory requirements, standards, and policies. Specific roles and responsibilities for the team include:  \* C+AI Security Assurance: This role is filled by security subject-matter experts (SMEs) from outside the project team. The Security Assurance team manages the SDL program and process within C+AI and conducts threat modeling sessions for project teams.  \* Compliance and Privacy Advisor: The advisor (or group of individuals) from the compliance team is responsible for attesting to compliance (or non-compliance) with security and privacy requirements without interference from the project team.  \* Team Champions: The team champion roles are filled by SMEs from the project team. These roles are responsible for the negotiation, acceptance, and tracking of minimum security and privacy requirements and maintaining clear lines of communication with advisors and decision makers during a service development project.  \* A training and awareness team responsible for educating project teams about security standards, policies, and best practices.  \* Help desk personnel to answer common questions and, as needed, escalate to the security and privacy SMEs.  \* Personnel responsible for authoring checklists, standards, and even corporate policy to meet security and privacy requirements.  \* Account management SME that acts as a liaison with application teams, manages the application portfolio, and ensures that the process for SDL compliance runs smoothly.  \* Remediation and risk management personnel, who both prioritize applications for assessment and manage the remediation of high-risk vulnerabilities found during the assessment.  \* The Operations team which conducts network and host scanning post-assessment across the enterprise and production servers. |
| **Part C**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for managing customer-deployed resources using a system development life cycle (SDLC), including the identification of individuals having information security and privacy roles and responsibilities.  **Azure**  Section 5 of this SSP refers to the individuals having Information Security roles and responsibilities. |
| **Part D**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for integrating the customer's information security risk management process into SDLC activities.  **Azure**  Azure integrates the organizational information security risk management process into the SDL process. Please see Part a above for details on how Azure’s SDL process facilitates the integration of the information security architecture with the organizational risk management. |

## SA-4 Acquisition Process

Include the following requirements, descriptions, and criteria, explicitly or by reference, using [Selection (OneOrMore): standardized contract language;[contract language is defined (if selected);] ] in the acquisition contract for the system, system component, or system service:

a. Security and privacy functional requirements;

b. Strength of mechanism requirements;

c. Security and privacy assurance requirements;

d. Controls needed to satisfy the security and privacy requirements.

e. Security and privacy documentation requirements;

f. Requirements for protecting security and privacy documentation;

g. Description of the system development environment and environment in which the system is intended to operate;

h. Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management; and

i. Acceptance criteria.

Requirement: The service provider must comply with Federal Acquisition Regulation (FAR) Subpart 7.103, and Section 889 of the John S. McCain National Defense Authorization Act (NDAA) for Fiscal Year 2019 (Pub. L. 115-232), and FAR Subpart 4.21, which implements Section 889 (as well as any added updates related to FISMA to address security concerns in the system acquisitions process).

Guidance: The use of Common Criteria (ISO/IEC 15408) evaluated products is strongly preferred. See https://www.niap-ccevs.org/Product/index.cfm or https://www.commoncriteriaportal.org/products/.

|  |
| --- |
| **SA-4 Control Summary Information** |
| Responsible Roles: SDL, CELA |
| Parameter sa-04\_odp.01: standardized contract language |
| Parameter sa-04\_odp.02: |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SA-4 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  The customer is responsible for implementing an acquisition process for customer-deployed resources that includes security and privacy functional requirements, strength of mechanism requirements, security and privacy assurance requirements, necessary controls to satisfy said security and privacy requirements, documentation requirements,  requirements for protecting security and privacy-related documentation, a description of the customer's development and operating environments, allocation of or identify of parties responsible for security, privacy, and supply chain risk management, and the acceptance criteria for the contract.  **Azure**  Azure implements the acquisitions control through enforcement of the Microsoft Security Policy (MSP). The Policy dictates that where a third party is allowed to (i) access, process, host or manage Microsoft’s online services’ information assets or information processing facilities, or (ii) add products or services to Microsoft’s online services’ information processing facilities, arrangements must be made in a formal contract to define responsibility and requirements for the security, confidentiality, integrity and availability of the information assets involved. Appropriate security and privacy standards are addressed in the agreement, to provide a level of protection against identified risks equivalent to that provided by the MSP.  It is the role of Corporate, External, and Legal Affairs (CELA) to require language included in system acquisition contracts pertaining to the security requirements, as appropriate, through the Master Supplier Services Agreement (MSSA) or an equivalent type of agreement. |
| **Part B**  **Customer Responsibility**  The customer is responsible for implementing an acquisition process for customer-deployed resources that includes security and privacy functional requirements, strength of mechanism requirements, security and privacy assurance requirements, necessary controls to satisfy said security and privacy requirements, documentation requirements,  requirements for protecting security and privacy-related documentation, a description of the customer's development and operating environments, allocation of or identify of parties responsible for security, privacy, and supply chain risk management, and the acceptance criteria for the contract.  **Azure**  Microsoft requires all device security documentation and tests all security requirements and functions in lab/development environments before implemented in production. Whenever feasible, Microsoft has selected system components and products that have been evaluated on Common Criteria, FIPS (e.g., Federal Information Processing Standards (FIPS) 140-2), Center for Information Security, Security Content Automation Protocol (SCAP) and other standards for deployment within Azure.  Microsoft engages only those third parties that have signed a contract and have been approved by the Procurement and Microsoft Corporate, External, and Legal Affairs (CELA) teams. In accordance with the MSSA, contracts require that the third party implement security procedures to prevent disclosure of Microsoft confidential information and provide all pertinent information describing the functional requirements or specifications of the security controls that are to be employed within the system. Additionally, third parties who have access to the Azure environment must employ a formal contract that defines the responsibilities and requirements for maintaining the security, confidentiality, integrity, and availability of the information assets involved with the contract. |
| **Part C**  **Customer Responsibility**  The customer is responsible for implementing an acquisition process for customer-deployed resources that includes security and privacy functional requirements, strength of mechanism requirements, security and privacy assurance requirements, necessary controls to satisfy said security and privacy requirements, documentation requirements,  requirements for protecting security and privacy-related documentation, a description of the customer's development and operating environments, allocation of or identify of parties responsible for security, privacy, and supply chain risk management, and the acceptance criteria for the contract.  **Azure**  Azure implements the acquisitions control through enforcement of the Microsoft Security Policy (MSP). The Policy dictates that where a third party is allowed to (i) access, process, host or manage Microsoft’s online services’ information assets or information processing facilities, or (ii) add products or services to Microsoft’s online services’ information processing facilities, arrangements must be made in a formal contract to define responsibility and requirements for the security, confidentiality, integrity and availability of the information assets involved. Appropriate security and privacy standards are addressed in the agreement, to provide a level of protection against identified risks equivalent to that provided by the MSP.  It is the role of Corporate, External, and Legal Affairs (CELA) to require language included in system acquisition contracts pertaining to the security requirements, as appropriate, through the Master Supplier Services Agreement (MSSA) or an equivalent type of agreement. |
| **Part D**  **Customer Responsibility**  The customer is responsible for implementing an acquisition process for customer-deployed resources that includes security and privacy functional requirements, strength of mechanism requirements, security and privacy assurance requirements, necessary controls to satisfy said security and privacy requirements, documentation requirements,  requirements for protecting security and privacy-related documentation, a description of the customer's development and operating environments, allocation of or identify of parties responsible for security, privacy, and supply chain risk management, and the acceptance criteria for the contract.  **Azure**  Azure implements the acquisitions control through enforcement of the Microsoft Security Policy (MSP). The Policy dictates that where a third party is allowed to (i) access, process, host or manage Microsoft’s online services’ information assets or information processing facilities, or (ii) add products or services to Microsoft’s online services’ information processing facilities, arrangements must be made in a formal contract to define responsibility and requirements for the security, confidentiality, integrity and availability of the information assets involved. Appropriate security and privacy standards are addressed in the agreement, to provide a level of protection against identified risks equivalent to that provided by the MSP.  It is the role of Corporate, External, and Legal Affairs (CELA) to require language included in system acquisition contracts pertaining to the security requirements, as appropriate, through the Master Supplier Services Agreement (MSSA) or an equivalent type of agreement. |
| **Part E**  **Customer Responsibility**  The customer is responsible for implementing an acquisition process for customer-deployed resources that includes security and privacy functional requirements, strength of mechanism requirements, security and privacy assurance requirements, necessary controls to satisfy said security and privacy requirements, documentation requirements,  requirements for protecting security and privacy-related documentation, a description of the customer's development and operating environments, allocation of or identify of parties responsible for security, privacy, and supply chain risk management, and the acceptance criteria for the contract.  **Azure**  Azure implements the acquisitions control through enforcement of the Microsoft Security Policy (MSP). The Policy dictates that where a third party is allowed to (i) access, process, host or manage Microsoft’s online services’ information assets or information processing facilities, or (ii) add products or services to Microsoft’s online services’ information processing facilities, arrangements must be made in a formal contract to define responsibility and requirements for the security, confidentiality, integrity and availability of the information assets involved. Appropriate security and privacy standards are addressed in the agreement, to provide a level of protection against identified risks equivalent to that provided by the MSP.  It is the role of Corporate, External, and Legal Affairs (CELA) to require language included in system acquisition contracts pertaining to the security requirements, as appropriate, through the Master Supplier Services Agreement (MSSA) or an equivalent type of agreement. |
| **Part F**  **Customer Responsibility**  The customer is responsible for implementing an acquisition process for customer-deployed resources that includes security and privacy functional requirements, strength of mechanism requirements, security and privacy assurance requirements, necessary controls to satisfy said security and privacy requirements, documentation requirements,  requirements for protecting security and privacy-related documentation, a description of the customer's development and operating environments, allocation of or identify of parties responsible for security, privacy, and supply chain risk management, and the acceptance criteria for the contract.  **Azure**  Azure implements the acquisitions control through enforcement of the Microsoft Security Policy (MSP). The Policy dictates that where a third party is allowed to (i) access, process, host or manage Microsoft’s online services’ information assets or information processing facilities, or (ii) add products or services to Microsoft’s online services’ information processing facilities, arrangements must be made in a formal contract to define responsibility and requirements for the security, confidentiality, integrity and availability of the information assets involved. Appropriate security and privacy standards are addressed in the agreement, to provide a level of protection against identified risks equivalent to that provided by the MSP.  It is the role of Corporate, External, and Legal Affairs (CELA) to require language included in system acquisition contracts pertaining to the security requirements, as appropriate, through the Master Supplier Services Agreement (MSSA) or an equivalent type of agreement. |
| **Part G**  **Customer Responsibility**  The customer is responsible for implementing an acquisition process for customer-deployed resources that includes security and privacy functional requirements, strength of mechanism requirements, security and privacy assurance requirements, necessary controls to satisfy said security and privacy requirements, documentation requirements,  requirements for protecting security and privacy-related documentation, a description of the customer's development and operating environments, allocation of or identify of parties responsible for security, privacy, and supply chain risk management, and the acceptance criteria for the contract.  **Azure**  Azure implements the acquisitions control through enforcement of the Microsoft Security Policy (MSP). The Policy dictates that where a third party is allowed to (i) access, process, host or manage Microsoft’s online services’ information assets or information processing facilities, or (ii) add products or services to Microsoft’s online services’ information processing facilities, arrangements must be made in a formal contract to define responsibility and requirements for the security, confidentiality, integrity and availability of the information assets involved. Appropriate security and privacy standards are addressed in the agreement, to provide a level of protection against identified risks equivalent to that provided by the MSP.  It is the role of Corporate, External, and Legal Affairs (CELA) to require language included in system acquisition contracts pertaining to the security requirements, as appropriate, through the Master Supplier Services Agreement (MSSA) or an equivalent type of agreement. |
| **Part H**  **Customer Responsibility**  The customer is responsible for implementing an acquisition process for customer-deployed resources that includes security and privacy functional requirements, strength of mechanism requirements, security and privacy assurance requirements, necessary controls to satisfy said security and privacy requirements, documentation requirements,  requirements for protecting security and privacy-related documentation, a description of the customer's development and operating environments, allocation of or identify of parties responsible for security, privacy, and supply chain risk management, and the acceptance criteria for the contract.  **Azure**  Azure implements the acquisitions control through enforcement of the Microsoft Security Policy (MSP). The Policy dictates that where a third party is allowed to (i) access, process, host or manage Microsoft’s online services’ information assets or information processing facilities, or (ii) add products or services to Microsoft’s online services’ information processing facilities, arrangements must be made in a formal contract to define responsibility and requirements for the security, confidentiality, integrity and availability of the information assets involved. Appropriate security and privacy standards are addressed in the agreement, to provide a level of protection against identified risks equivalent to that provided by the MSP.  It is the role of Corporate, External, and Legal Affairs (CELA) to require language included in system acquisition contracts pertaining to the security requirements, as appropriate, through the Master Supplier Services Agreement (MSSA) or an equivalent type of agreement. |
| **Part I**  **Customer Responsibility**  The customer is responsible for implementing an acquisition process for customer-deployed resources that includes security and privacy functional requirements, strength of mechanism requirements, security and privacy assurance requirements, necessary controls to satisfy said security and privacy requirements, documentation requirements,  requirements for protecting security and privacy-related documentation, a description of the customer's development and operating environments, allocation of or identify of parties responsible for security, privacy, and supply chain risk management, and the acceptance criteria for the contract.  **Azure**  Azure implements the acquisitions control through enforcement of the Microsoft Security Policy (MSP). The Policy dictates that where a third party is allowed to (i) access, process, host or manage Microsoft’s online services’ information assets or information processing facilities, or (ii) add products or services to Microsoft’s online services’ information processing facilities, arrangements must be made in a formal contract to define responsibility and requirements for the security, confidentiality, integrity and availability of the information assets involved. Appropriate security and privacy standards are addressed in the agreement, to provide a level of protection against identified risks equivalent to that provided by the MSP.  It is the role of Corporate, External, and Legal Affairs (CELA) to require language included in system acquisition contracts pertaining to the security requirements, as appropriate, through the Master Supplier Services Agreement (MSSA) or an equivalent type of agreement. |

### SA-4(1) - Functional Properties of Controls

Require the developer of the system, system component, or system service to provide a description of the functional properties of the controls to be implemented.

|  |
| --- |
| **SA-4(1) Control Summary Information** |
| Responsible Roles: CELA |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SA-4(1) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for obtaining a description of the functional properties of security controls to be employed from the developer of the corresponding customer-deployed resource(s). Note: Azure hosts the customer-deployed system. The customer can find a description of the security controls employed by Azure below.  **Azure**  The acquisition process includes contractual requirements to provide documentation of security functionality. Documentation provided in response to this requirement is stored by Azure service teams in their internal SharePoint sites. |

### SA-4(2) - Design and Implementation Information for Controls

Require the developer of the system, system component, or system service to provide design and implementation information for the controls that includes: [Selection (OneOrMore): security-relevant external system interfaces;high-level design;low-level design;source code or hardware schematics;[design and implementation information is defined (if selected);] ] at [level of detail is defined;].

|  |
| --- |
| **SA-4(2) Control Summary Information** |
| Responsible Roles: SDL, CELA |
| Parameter sa-04.02\_odp.01: security-relevant external system interfaces; high-level design; design and implementation information required by the SDL process |
| Parameter sa-04.02\_odp.02: |
| Parameter sa-04.02\_odp.03: a level of detail sufficient for secure deployment |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SA-4(2) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for obtaining design and implementation information for the security controls to be employed from the developer of the corresponding customer-deployed resource(s), that includes: security-relevant external system interfaces; high-level design; low-level design; source code schematics; and any customer-defined design/implementation information at an organization-defined level of detail in the design and implementation information. Note: Azure hosts the customer-deployed system. The customer can find a description of the security controls employed by Azure below.  **Azure**  The acquisition process includes contractual requirements to provide documentation of security functionality, including security-relevant external system interfaces and high-level design. Documentation provided in response to this requirement is stored by Azure service teams in their internal SharePoint sites. |

### SA-4(5) - System, Component, and Service Configurations

Require the developer of the system, system component, or system service to:

(a) Deliver the system, component, or service with [The service provider shall use the DoD STIGs to establish configuration settings; Center for Internet Security up to Level 2 (CIS Level 2) guidelines shall be used if STIGs are not available; Custom baselines shall be used if CIS is not available.] implemented; and

(b) Use the configurations as the default for any subsequent system, component, or service reinstallation or upgrade.

|  |
| --- |
| **SA-4(5) Control Summary Information** |
| Responsible Roles: SDL |
| Parameter sa-04.05\_odp: The service provider shall use the DoD STIGs to establish configuration settings; Center for Internet Security up to Level 2 (CIS Level 2) guidelines shall be used if STIGs are not available; Custom baselines shall be used if CIS is not available. |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SA-4(5) What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  The customer is responsible for requiring the developer of the information system, system component, or information system service to deliver the system, component, or service with organization-defined security configurations implemented.  **Azure**  Azure ensures consistent and required configurations applied through both Azure Security Pack (AzSecPack) implementations and the Security Development Lifecycle (SDL). AzSecPack ensures the application and enforcement of the Azure security baseline, which is based on a hyperscale-compatible subset of DISA STIG and CIS Benchmark requirements. The SDL ensures that any Microsoft-authored code complies with scanning and code requirements. |
| **Part B**  **Customer Responsibility**  The customer is responsible for requiring the developer of the information system, system component, or information system service to use the configurations as the default for any subsequent system, component, or service reinstallation or upgrade.  **Azure**  Azure ensures consistent and required configurations applied through both Azure Security Pack (AzSecPack) implementations and the Security Development Lifecycle (SDL). System, component, and service reinstallation and upgrade are handled through the same processes, ensuring consistency of baselines. |

### SA-4(9) - Functions, Ports, Protocols, and Services in Use

Require the developer of the system, system component, or system service to identify the functions, ports, protocols, and services intended for organizational use.

|  |
| --- |
| **SA-4(9) Control Summary Information** |
| Responsible Roles: Logging and Monitoring, SDL |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SA-4(9) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for obtaining a plan for continuously monitoring security control effectiveness from the developer of the corresponding customer-deployed resource(s). Note: Azure hosts the customer-deployed system. The customer can find a description of the security controls employed by Azure below.  **Azure**  Azure follows the Security Development Lifecycle (SDL) process, which includes as part of the design phase the identification of the functions, ports, protocols, and services intended for organizational use. |

### SA-4(10) - Use of Approved PIV Products

Employ only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational systems.

|  |
| --- |
| **SA-4(10) Control Summary Information** |
| Responsible Roles: Azure Compliance |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☒ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☒ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SA-4(10) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for employing FIPS 201-approved technology products to support Personal Identity Verification (PIV) capability. Note: if the customer does not deploy PIV credentials this control is not applicable.  **Azure**  Azure does not utilize Personal Identity Verification (PIV) credentials for internal personnel because PIV cards are not available to Azure. |

## SA-5 System Documentation

a. Obtain or develop administrator documentation for the system, system component, or system service that describes:

1. Secure configuration, installation, and operation of the system, component, or service;

2. Effective use and maintenance of security and privacy functions and mechanisms; and

3. Known vulnerabilities regarding configuration and use of administrative or privileged functions;

b. Obtain or develop user documentation for the system, system component, or system service that describes:

1. User-accessible security and privacy functions and mechanisms and how to effectively use those functions and mechanisms;

2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner and protect individual privacy; and

3. User responsibilities in maintaining the security of the system, component, or service and privacy of individuals;

c. Document attempts to obtain system, system component, or system service documentation when such documentation is either unavailable or nonexistent and take [actions to take when system, system component, or system service documentation is either unavailable or nonexistent are defined;] in response; and

d. Distribute documentation to [at a minimum, the ISSO (or similar role within the organization)].

|  |
| --- |
| **SA-5 Control Summary Information** |
| Responsible Roles: SDL |
| Parameter sa-05\_odp.01: action to create such documentation for internal use |
| Parameter sa-05\_odp.02: service team roles responsible for security implementations |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SA-5 What is the solution and how is it implemented?** |
| **Part A1**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for obtaining or developing administrator documentation for customer-deployed resources that describes secure configuration, installation, and operation of the customer-deployed resources.  **Azure**  Azure service teams maintain, secure, manage, and store information system documentation, including documentation regarding secure configuration, installation, and operation of the Azure cloud. This documentation is stored in each service team’s SharePoint site or internal Microsoft website such as KnowledgeBase and made available to service team members.  Microsoft ensures the appropriate service team maintains, secures, manages, transmits and stores all service-specific documentation to prevent unauthorized access and misuse. Microsoft considers all documentation to be categorized as a system asset. The service team is responsible for classifying its assets and employing the associated safeguards according to the Asset Classification Standard and Asset Protection Standard, as well as any additional requirements defined by the service team. An asset is something that supports the delivery of the Azure service or has other business value to its internal Microsoft owner.  The service's documentation inventory is located on the team SharePoint site or internal Microsoft website such as KnowledgeBase. The inventory of such document assets is maintained by service team Technical Support personnel and is updated as needed when new assets are created, installed or identified or the asset owner, location or security classification requires modification. |
| **Part A2**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for obtaining or developing administrator documentation for customer-deployed resources that describes effective use and maintenance of security and privacy functions/mechanisms.  **Azure**  Azure service teams maintain, secure, manage, and store information system documentation, including documentation regarding effective use and maintenance of security and privacy features/functions of the Azure cloud. This documentation is stored in each service team’s SharePoint site or internal Microsoft website such as KnowledgeBase and made available to service team members.  Service team documentation, including but not limited to Standard Operating Procedures and Troubleshooting Guides (TSGs), are stored on each team’s respective SharePoint site or internal Microsoft website such as KnowledgeBase as referenced in each team’s asset inventory. Authorized service team personnel routinely develop, maintain and store all related security documentation (e.g., security policies and procedures) and system configuration files on a continuous basis in accordance with regulatory requirements. Documentation is centrally managed and available to only authorized personnel using role-based access. |
| **Part A3**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for obtaining or developing administrator documentation for customer-deployed resources that describes known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions.  **Azure**  Azure service teams maintain, secure, manage, and store information system documentation, including documentation regarding known vulnerabilities regarding configuration and use of administrative (i.e. privileged) functions. Known vulnerabilities are identified in the assessment results and Plans of Action and Milestones (POA&Ms) as part of the Security Authorization package and maintained on the SharePoint site with the Azure Security Authorization documentation. |
| **Part B1**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for obtaining or developing user documentation for customer-deployed resources that describes user-accessible security and privacy functions/mechanisms and how to effectively use them.  **Azure**  Azure has extensive user-facing documentation on all aspects of the system, including security and privacy functions and their use. This documentation is available online at the following address:  <https://learn.microsoft.com/en-us/azure/> |
| **Part B2**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for obtaining or developing user documentation for customer-deployed resources that describes methods for user interaction, which enables individuals to use the customer-deployed resources in a more secure manner and protect individual privacy.  **Azure**  Azure has extensive user-facing documentation on all aspects of the system, including methods for user interaction. This documentation is available online at the following address:  <https://learn.microsoft.com/en-us/azure/> |
| **Part B3**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for obtaining or developing user documentation for customer-deployed resources that describes user responsibilities in maintaining the security of the customer-deployed resources and privacy of individuals.  **Azure**  Azure has extensive user-facing documentation on all aspects of the system, including maintaining the security of the service's resources and the privacy of individuals. This documentation is available online at the following address:  <https://learn.microsoft.com/en-us/azure/> |
| **Part C**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for documenting and taking customer-defined actions in response to attempts to obtain administrator and/or user documentation for customer-deployed resources when such documentation is not available/nonexistent.  **Azure**  Azure addresses attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent with preventive and detective measures. As a preventive measure, Azure requires only current software to be installed in the environment. The only operating system and server application software versions allowed in Azure datacenters are approved current versions, approved legacy versions, and approved pre-release versions. In the case there is an inability to obtain needed documentation due to the age of the information system/component, the organization would track those needs via the Microsoft Operations Center (MOC). As a detective measure, the MOC maintains Troubleshooting Guides (TSGs) to address issues in the Azure environment with physical and virtual assets. These TSGs include low level design details to allow for Microsoft personnel to effectively analyze assets. The TSGs are widely available to all users of the environment; however, sensitive information (i.e. system architecture) is stored separately and requires user login/password to access. Access to the sensitive information is restricted to only MOC personnel. Documentation for externally-provided software (scanning tools) is available online at vendor websites. |
| **Part D**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for distributing documentation for customer-deployed resources identified in SA-05.a, SA-05.b and SA-05.c are distributed to customer-defined personnel/roles.  **Azure**  This documentation is stored in each service team’s SharePoint site and made available to service team members. The documentation is secured via SharePoint's internal security mechanisms. Information system documentation is distributed to only the appropriate groups and individuals on a need to know basis and is based on job responsibilities.  Documentation for externally-provided software (scanning tools) is available online at vendor websites. |

## SA-8 Security and Privacy Engineering Principles

Apply the following systems security and privacy engineering principles in the specification, design, development, implementation, and modification of the system and system components: [Assignment: organization-defined systems security and privacy engineering principles].

|  |
| --- |
| **SA-8 Control Summary Information** |
| Responsible Roles: SDL |
| Parameter sa-8: organization-defined systems security and privacy engineering principles |
| Parameter sa-08\_odp.01: |
| Parameter sa-08\_odp.02: |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SA-8 What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for applying security and privacy engineering principles in the specification, design, development, implementation, and modification of customer-deployed resources.  **Azure**  Azure has a mature Security Development Lifecycle (SDL) process that is followed for all engineering and development projects. The Microsoft SDL process includes the following phases which implement standard security and privacy engineering principles across all of Microsoft’s online services:  \* Phase 1: Requirements - The Requirements phase of the SDL includes the project inception—when the organization considers security and privacy at a foundational level—and a cost analysis—when determining if development and support costs for improving security and privacy are consistent with business needs. This phase also includes defining security roles and responsibilities and identifying individuals with these roles and responsibilities.  \* Phase 2: Design - The Design phase is when the organization builds the plan for how to take the project through the rest of the SDL process—from implementation, to verification, to release. During the Design phase the organization establishes best practices to follow for this phase by way of functional and design specifications, and by performing risk analysis to identify threats and vulnerabilities in the software. TMA (Threat Model Analysis) is required to define all attack surfaces and their associated risks; all security gaps and risks and documented and analyzed. This security impact analysis results in dataflow documentation in order to identify all intended paths for information and potential attack vectors.  \* Phase 3: Implementation - The Implementation phase is when the organization creates the documentation and tools the customer uses to make informed decisions about how to deploy the software securely. To this end, the Implementation phase is when the organization establishes development best practices to detect and remove security and privacy issues early in the development cycle. Microsoft understands, observes, and implements the security requirements and considerations as outlined in GSA IT Security Procedural Guide 09-48, Security Language for IT Acquisition Efforts, dated September 2009 for the information system consistent with the Azure offering’s requirements.  \* Phase 4: Verification - During the Verification phase, the organization ensures that the code meets the security and privacy tenets established in the previous phases. This is done through security and privacy testing, and a security push—which is a team-wide focus on threat model updates, code review, testing, and thorough documentation review and edit. Additionally, service teams create a Security Incident Management document as part of their SDL requirements that outlines how security-specific incidents are addressed. A public release privacy review is also completed during the Verification phase.  \* Phase 5: Release - The Release phase is when the organization prepares the software for consumption and prepares for what happens once the software is released. One of the core concepts in the Release phase is response planning—mapping out a plan of action, should any security or privacy vulnerabilities be discovered in the release—and this carries over to post-release, as well, in terms of response execution. To this end, a Final Security Review and privacy review is required prior to release.  The SDL dashboard is used to monitor the progress of all engineering initiatives and controls the process to ensure that all steps are followed. The System Owner is responsible for ensuring that the SDL process is followed for all engineering initiatives associated with Azure. |

## SA-9 External System Services

a. Require that providers of external system services comply with organizational security and privacy requirements and employ the following controls: [Appropriate FedRAMP Security Controls Baseline (s) if Federal information is processed or stored within the external system];

b. Define and document organizational oversight and user roles and responsibilities with regard to external system services; and

c. Employ the following processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis: [Federal/FedRAMP Continuous Monitoring requirements must be met for external systems where Federal information is processed or stored].

|  |
| --- |
| **SA-9 Control Summary Information** |
| Responsible Roles: Azure Compliance |
| Parameter sa-09\_odp.01: FedRAMP Security Controls Baselines if Federal information is processed or stored within the external system |
| Parameter sa-09\_odp.02: Federal/FedRAMP Continuous Monitoring requirements must be met for external systems where Federal information is processed or stored |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SA-9 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for requiring that external service providers comply with the customer's information security and privacy requirements and employ customer-defined security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.  **Azure**  Azure is owned and operated by Microsoft; there are no external information system services involved in the delivery of Azure services.  However, if Azure does utilize external information system services outside of the Azure authorization boundary, it ensures that they comply with the information security requirements. Subsequent changes are coordinated with the FedRAMP JAB, DISA/DoD authorizing officials, and other regulators as required to determine if it signifies a major change; and update documentation and reauthorize as needed per direction from the FedRAMP JAB, DISA/DoD authorizing officials, and other regulators as required.  Additionally, Microsoft provides deliverables to the FedRAMP JAB, DISA/DoD authorizing officials, and other regulators as required as part of continuous monitoring activities allowing sufficient Government oversight. Microsoft follows the standard process outlined below in the event it does utilize services outside of the Azure authorization boundary.  Microsoft engages Vendor Agencies through Microsoft’s third party ordering tool, which is designed for third parties (Vendor Agencies) that have signed a Master Supplier Services Agreement (MSSA) and/or have been approved by the Global Procurement Group (GPG) as an “Approved Vendor” in specific categories of work. GPG requires the third party to comply with all applicable Microsoft security policies and implement security procedures to prevent disclosure of Microsoft Confidential information. Microsoft includes provisions in the MSSA and any associated Statements of Work (SOW) with each vendor addressing the need to employ appropriate security controls. Additionally, vendors that handle high business impact data must be in annual compliance with the Microsoft Supplier Security and Privacy Assurance (SSPA) Program Guide. |
| **Part B**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for defining and documenting government oversight and user responsibilities and roles with regard to external system services.  **Azure**  Azure signs ISAs with external information systems; ISAs define Azure oversight and roles/responsibilities. Agencies receive and review ISAs as part of their authorization decision. Government oversight is performed by this agency review of Azure ISAs and continuous monitoring, which includes reports on ISA oversight. |
| **Part C**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for continuously monitoring external service providers through customer-defined processes, methods, and techniques.  **Azure**  Azure monitoring processes, methods and techniques are applied to customer data and access control data and are documented in ISAs and executed by Azure Security. |

### SA-9(1) - Risk Assessments and Organizational Approvals

(a) Conduct an organizational assessment of risk prior to the acquisition or outsourcing of information security services; and

(b) Verify that the acquisition or outsourcing of dedicated information security services is approved by [personnel or roles that approve the acquisition or outsourcing of dedicated information security services is/are defined;].

|  |
| --- |
| **SA-9(1) Control Summary Information** |
| Responsible Roles: Azure Compliance |
| Parameter sa-09.01\_odp: FedRAMP Joint Authorization Board and/or the DoD Component CIO or their delegate(s) |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SA-9(1) What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for conducting a risk assessment prior to acquiring or outsourcing dedicated information security services.  **Azure**  Azure is owned and operated by Microsoft; there are no external information system services involved in the delivery of Azure services. Azure does not consider any information security services to be outsourced as they are defined in the supplemental guidance for this requirement. If any services were to be outsourced after receiving an ATO, Azure Security would complete an assessment of risk and follow approved change management processes, including integration with the Significant Change Request (SCR) process with Azure's compliance team. |
| **Part B**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for obtaining approval of acquisitions or outsourcing of dedicated information security services.  **Azure**  Azure ensures the acquisition or outsourcing of dedicated information security services is approved by the FedRAMP JAB, DISA/DoD authorizing officials, and other regulators. |

### SA-9(2) - Identification of Functions, Ports, Protocols, and Services

Require providers of the following external system services to identify the functions, ports, protocols, and other services required for the use of such services: [all external systems where Federal information is processed or stored].

|  |
| --- |
| **SA-9(2) Control Summary Information** |
| Responsible Roles: Azure Compliance |
| Parameter sa-09.02\_odp: all external systems where Federal information is processed or stored |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SA-9(2) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for requiring external service providers to identify the functions, ports, protocols and other services required for the use of that service.  **Azure**  Azure is owned and operated by Microsoft; there are no external information system services involved in the delivery of Azure services. Azure does not consider any information security services to be outsourced as they are defined in the supplemental guidance for this requirement. If any services were to be outsourced after receiving an ATO, Azure Security would complete an assessment of risk and follow approved change management processes, including integration with the Significant Change Request (SCR) process with Azure's compliance team. |

### SA-9(5) - Processing, Storage, and Service Location

Restrict the location of [Selection (OneOrMore): information processing;information or data;system services] to [U.S./U.S. Territories or geographic locations where there is U.S. jurisdiction] based on [all High impact data, systems, or services].

|  |
| --- |
| **SA-9(5) Control Summary Information** |
| Responsible Roles: Datacenter Hosting |
| Parameter sa-09.05\_odp.01: information processing, information data, and information services |
| Parameter sa-09.05\_odp.02: Azure continental United States datacenters |
| Parameter sa-09.05\_odp.03: Azure business requirements |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SA-9(5) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for restricting the location of information processing, storage, and service.  **Azure**  Azure restricts the location of all services and data within the accreditation boundary to Azure continental United States datacenters. |

## SA-10 Developer Configuration Management

Require the developer of the system, system component, or system service to:

a. Perform configuration management during system, component, or service [Selection (OneOrMore): design;development;implementation;operation;disposal] ;

b. Document, manage, and control the integrity of changes to [configuration items under configuration management are defined;];

c. Implement only organization-approved changes to the system, component, or service;

d. Document approved changes to the system, component, or service and the potential security and privacy impacts of such changes; and

e. Track security flaws and flaw resolution within the system, component, or service and report findings to [personnel to whom security flaws and flaw resolutions within the system, component, or service are reported is/are defined;].

(e) Requirement: track security flaws and flaw resolution within the system, component, or service and report findings to organization-defined personnel, to include FedRAMP.

|  |
| --- |
| **SA-10 Control Summary Information** |
| Responsible Roles: SDL |
| Parameter sa-10\_odp.01: development, implementation, and operation |
| Parameter sa-10\_odp.02: configuration items identified in CM-03 |
| Parameter sa-10\_odp.03: Azure Security Operations |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SA-10 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for requiring the developer of customer-deployed resources to perform configuration management during the design, development, implementation, operation, and disposal of the resources provided.  **Azure**  All Azure software developers are required to follow the Azure Configuration Management Plan (CMP) and Microsoft’s Security Development Lifecycle (SDL) during information system design, development, implementation, operation, and disposal. |
| **Part B**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for requiring the developer of customer-deployed resources to document, manage, and control the integrity of changes to customer-defined configuration items.  **Azure**  Azure developers leverage Git or Azure DevOps to document, manage and control the integrity of changes in the development environment. These tools provide technical enforcement of documented change management processes and the SDL. Among other features, they prevent changes to configuration items that are not tied to an approved change request. |
| **Part C**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for requiring the developer of customer-deployed resources to utilize configuration management such that the developer implements only organization-approved changes to the resources provided.  **Azure**  Developers of Azure implement only approved changes to the system. The service teams follow the configuration management processes when implementing changes. Changes are approved through Git or Azure DevOps. |
| **Part D**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for requiring the developer of customer-deployed resources to utilize configuration management and to document approved changes and the potential security and privacy impacts of such changes.  **Azure**  The service team tracks all approved changes in Git or Azure DevOps. The software build services of GIT and Azure DevOps have configurations in place to ensure the approval of changes by at least one other reviewer other than the individual who developed the change prior to deployment into the Azure production environment. In addition, proper testing is conducted for the changes prior to being deployed to production. As part of these change management processes, other documentation such as the SSP or user and administrative documentation is updated if applicable. |
| **Part E**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for requiring the developer of customer-deployed resources to utilize configuration management, including tracking security flaws through resolution and reporting findings to customer-defined personnel.  **Azure**  Azure service team developers track security flaws and flaw resolution during the development process using Azure DevOps. Any identified flaws, whether discovered by a human or by the automated tools, have a corresponding bug opened in Azure DevOps. The resolution of the flaw is then documented and tracked using the bug. A summary of identified flaws and their resolution is provided to service team management, Azure Security, and authorizing officials. |

## SA-11 Developer Testing and Evaluation

Require the developer of the system, system component, or system service, at all post-design stages of the system development life cycle, to:

a. Develop and implement a plan for ongoing security and privacy control assessments;

b. Perform [Selection (OneOrMore): unit;integration;system;regression] testing/evaluation [frequency at which to conduct {{ insert: param, sa-11\_odp.01 }} testing/evaluation is defined;] at [depth and coverage of {{ insert: param, sa-11\_odp.01 }} testing/evaluation is defined;];

c. Produce evidence of the execution of the assessment plan and the results of the testing and evaluation;

d. Implement a verifiable flaw remediation process; and

e. Correct flaws identified during testing and evaluation.

|  |
| --- |
| **SA-11 Control Summary Information** |
| Responsible Roles: SDL |
| Parameter sa-11\_odp.01: tests required by the SDL process |
| Parameter sa-11\_odp.02: organization-defined frequency |
| Parameter sa-11\_odp.03: depth and coverage required by the SDL process |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SA-11 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for requiring the developer of customer-deployed resources to develop and implement a plan for ongoing security and privacy control assessments.  **Azure**  Azure develops security and privacy control assessment plans in accordance with Microsoft's Security Development Lifecycle (SDL) process. Security testing occurs during the following phases of the process:  \* Phase 3 – Implementation  \* Phase 4 – Verification  \* Phase 5 – Release |
| **Part B**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for requiring the developer of customer-deployed resources to perform unit, integration, system, and/or regression testing/evaluation at the customer-defined depth and coverage.  **Azure**  Azure develops security assessment plans in accordance with Microsoft's Security Development Lifecycle (SDL) process. |
| **Part C**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for requiring the developer of customer-deployed resources to produce evidence of assessment plan execution and the results of testing/evaluation.  **Azure**  The results of the security tests are documented in tickets opened in Azure DevOps. Remediation work and successful retesting is documented in the same ticket. |
| **Part D**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for requiring the developer of customer-deployed resources to perform testing and evaluation, including implementing a verifiable flaw remediation process.  **Azure**  The Azure system owner is responsible for ensuring that all system development and maintenance activities are performed in accordance with the Microsoft SDL process.  A formal review process is implemented to ensure that new or modified source code authored by Microsoft’s online services staff is developed in a secure fashion, no malicious code has been introduced into the system, and that proper coding practices are followed. The reviewers’ names, review dates, and review results are documented in Azure DevOps, and maintained for audit purposes.  A formal security quality assurance process is implemented to test for vulnerabilities to known security exposures and exploits. The process includes the use of automated security testing tools and requires that all vulnerabilities are remediated in accordance with the SDL BugBar. A ticket for each vulnerability is opened in Azure DevOps and tracked to resolution. |
| **Part E**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for requiring the developer of customer-deployed resources to perform testing and evaluation, including the correction of flaws identified during security testing/evaluation.  **Azure**  As part of the SDL process, flaws identified during testing are remediated prior to release. The results of the security tests are documented in tickets opened in Azure DevOps. Remediation work and successful retesting is documented in the same ticket. |

### SA-11(1) - Static Code Analysis

Require the developer of the system, system component, or system service to employ static code analysis tools to identify common flaws and document the results of the analysis.

Requirement: The service provider must document its methodology for reviewing newly developed code for the Service in its Continuous Monitoring Plan. If Static code analysis cannot be performed (for example, when the source code is not available), then dynamic code analysis must be performed (see SA-11 (8))

|  |
| --- |
| **SA-11(1) Control Summary Information** |
| Responsible Roles: SDL |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SA-11(1) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for requiring the developer of customer-deployed resources to employ static code analysis tools to identify common flaws and document the results of the analysis.  **Azure**  Code reviews are performed as part of the Security Development Lifecycle (SDL), including using automated static code analysis tools. All release builds are run through virus scanning checks and the results are resolved prior to release into production. Automated code analysis tools such as BinSkim, Credential Scanner (CredScan), and other tools are run as determined by the SDL requirements. CredScan is utilized on all official builds in all build pipelines, and either breaking the build process preventing production use or creating work items assigned to the Azure service team for remediation. Virus and malware identification is run on all builds in all pipelines, and it breaks the build if issues are found. |

### SA-11(2) - Threat Modeling and Vulnerability Analyses

Require the developer of the system, system component, or system service to perform threat modeling and vulnerability analyses during development and the subsequent testing and evaluation of the system, component, or service that:

(a) Uses the following contextual information: [information concerning impact, environment of operations, known or assumed threats, and acceptable risk levels to be used as contextual information for threat modeling and vulnerability analyses is defined;];

(b) Employs the following tools and methods: [the tools and methods to be employed for threat modeling and vulnerability analyses are defined;];

(c) Conducts the modeling and analyses at the following level of rigor: [Assignment: organization-defined breadth and depth of modeling and analyses] ; and

(d) Produces evidence that meets the following acceptance criteria: [Assignment: organization-defined acceptance criteria].

|  |
| --- |
| **SA-11(2) Control Summary Information** |
| Responsible Roles: SDL |
| Parameter sa-11.2\_prm\_3: organization-defined breadth and depth of modeling and analyses |
| Parameter sa-11.2\_prm\_4: organization-defined acceptance criteria |
| Parameter sa-11.02\_odp.01: information |
| Parameter sa-11.02\_odp.02: tools and methods |
| Parameter sa-11.02\_odp.03: |
| Parameter sa-11.02\_odp.04: |
| Parameter sa-11.02\_odp.05: |
| Parameter sa-11.02\_odp.06: |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SA-11(2) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for requiring the developer of customer-deployed resources to perform testing and evaluation, including threat and vulnerability analyses and subsequent testing/evaluation of the as-built resources.  **Azure**  In accordance with Microsoft’s Security Development Lifecycle (SDL), security testing occurs in several phases throughout the SDL process. Specifically, security testing occurs during the following phases:  \* Phase 3 – Implementation  \* Phase 4 – Verification  \* Phase 5 – Release  Testing at the release phase is performed on the as-built system. Vulnerabilities found at the release testing phase are tracked and remediated. |

## SA-15 Development Process, Standards, and Tools

a. Require the developer of the system, system component, or system service to follow a documented development process that:

1. Explicitly addresses security and privacy requirements;

2. Identifies the standards and tools used in the development process;

3. Documents the specific tool options and tool configurations used in the development process; and

4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and

b. Review the development process, standards, tools, tool options, and tool configurations [frequency as before first use and annually thereafter] to determine if the process, standards, tools, tool options and tool configurations selected and employed can satisfy the following security and privacy requirements: [Assignment: organization-defined security and privacy requirements].

|  |
| --- |
| **SA-15 Control Summary Information** |
| Responsible Roles: SDL |
| Parameter sa-15(b): security and privacy requirements defined by Microsoft |
| Parameter sa-15\_odp.01: as needed and as dictated by the current threat posture |
| Parameter sa-15\_odp.02: |
| Parameter sa-15\_odp.03: |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SA-15 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for requiring developers of customer-deployed resources to follow a documented development process that: explicitly addresses security and privacy requirements; identifies standards and tools used; documents the specific tool options and configurations used; documents, manages, and ensures the integrity of changes to the process and/or tools used in development.  **Azure**  All development in Azure must follow the Security Development Lifecycle (SDL) process for all engineering and development projects. The SDL process includes the following:  \* Addressing security requirements: The Requirements phase of the SDL includes the project inception—when the organization considers security and privacy at a foundational level—and a cost analysis—when determining if development and support costs for improving security and privacy are consistent with business needs.  \* Identifying standards and tools/documents tools and configurations: The Implementation phase is when the organization creates the documentation and tools the customer uses to make informed decisions about how to deploy the software securely. To this end, the Implementation phase is when the organization establishes development best practices to detect and remove security and privacy issues early in the development cycle. Microsoft understands, observes, and implements the security requirements and considerations as outlined in GSA IT Security Procedural Guide 09-48, Security Language for IT Acquisition Efforts for the information system consistent with the Azure offering’s requirements.  \* Documents, manages, and ensures the integrity of changes: During the Verification phase, the organization ensures that the code meets the security and privacy tenets established in the previous phases. This is done through security and privacy testing, and a security push—which is a team-wide focus on threat model updates, code review, testing, and thorough documentation review and edit. A public release privacy review is also completed during the Verification phase. |
| **Part B**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for reviewing the development process, standards, tools, and tool options/configurations as needed to determine if they can satisfy security and privacy requirements.  **Azure**  Microsoft reviews the SDL process at least every six months to ensure that the process, standards, and tools selected and employed provide sufficient security and privacy for all services and software developed and released by Microsoft. |

### SA-15(3) - Criticality Analysis

Require the developer of the system, system component, or system service to perform a criticality analysis:

(a) At the following decision points in the system development life cycle: [decision points in the system development life cycle are defined;] ; and

(b) At the following level of rigor: [Assignment: organization-defined breadth and depth of criticality analysis].

|  |
| --- |
| **SA-15(3) Control Summary Information** |
| Responsible Roles: SDL |
| Parameter sa-15.3\_prm\_2: organization-defined breadth/depth |
| Parameter sa-15.03\_odp.01: at least every six (6) months |
| Parameter sa-15.03\_odp.02: |
| Parameter sa-15.03\_odp.03: |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SA-15(3) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for requiring the developer of the information system, system component, or information system service to perform a criticality analysis at an organization-defined breadth/depth and at organization-defined decision points in the system development life cycle.  **Azure**  Microsoft reviews the SDL process at least every six (6) months to ensure that the process, standards, and tools selected and employed provide sufficient security for all services developed and released by Microsoft. |

## SA-16 Developer-provided Training

Require the developer of the system, system component, or system service to provide the following training on the correct use and operation of the implemented security and privacy functions, controls, and/or mechanisms: [training on the correct use and operation of the implemented security and privacy functions, controls, and/or mechanisms provided by the developer of the system, system component, or system service is defined;].

|  |
| --- |
| **SA-16 Control Summary Information** |
| Responsible Roles: Training |
| Parameter sa-16: initial, ongoing, and annual training to include review of system documentation created by service teams and stored in team SharePoint sites |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SA-16 What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for requiring the developer of customer-deployed resources to provide customer-defined training on the correct use and operation of the implemented security functions, controls, and/or mechanisms for the resources provided.  **Azure**  All members of software development teams receive appropriate training to stay informed about security basics and recent trends in security. Individuals who develop software programs are required to complete at least one security training course in person or online each year. Security training can help ensure software is created with security in mind and can also help development teams stay current on security issues. Project team members are strongly encouraged to seek additional security and privacy education that is appropriate to their needs or products.  Azure service teams maintain, secure, manage, and store information system documentation, including documentation regarding:  \* Secure configuration, installation, and operation of the information system;  \* Effective use and maintenance of security features/functions; and  \* Known vulnerabilities regarding configuration and use of administrative (i.e. elevated) functions  This documentation is stored in each service team’s SharePoint site through Azure Security and is made available to service team members. Review of relevant documentation is part of initial and ongoing training activities held at least annually. |

## SA-17 Developer Security and Privacy Architecture and Design

Require the developer of the system, system component, or system service to produce a design specification and security and privacy architecture that:

a. Is consistent with the organization's security and privacy architecture that is an integral part the organization's enterprise architecture;

b. Accurately and completely describes the required security and privacy functionality, and the allocation of controls among physical and logical components; and

c. Expresses how individual security and privacy functions, mechanisms, and services work together to provide required security and privacy capabilities and a unified approach to protection.

|  |
| --- |
| **SA-17 Control Summary Information** |
| Responsible Roles: SDL |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SA-17 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for requiring the developer of customer-deployed resources to produce a design specification and security and privacy architecture that is consistent with and supportive of the customer's enterprise architecture.  **Azure**  Microsoft's software development practices include evaluating the design, security and privacy architecture of new services and components in the environment. The C+AI Security Assurance team works with the component/feature teams to provide guidance during the implementation of Security Development Lifecycle (SDL) activities in software development projects including identifying requirements for deep review such as threat modeling, and penetration testing. |
| **Part B**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for requiring the developer of customer-deployed resources to produce a design specification and security and privacy architecture that accurately and completely describes the required security functionality, and the allocation of security and privacy controls among logical resources.  **Azure**  The security and privacy architecture produced during the Design phase of the SDL process defines all attack surfaces, their associated risks, and security and privacy functionality necessary to address those risks. |
| **Part C**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for requiring the developer of customer-deployed resources to produce a design specification and security and privacy architecture that expresses how individual security and privacy functions, mechanisms, and services work together to provide required security and privacy capabilities and a unified approach to protection.  **Azure**  The security and privacy architecture produced during the Design phase of the SDL process demonstrates how individual security and privacy functions reinforce each other to provide a complete and unified approach to protection. |

## SA-21 Developer Screening

Require that the developer of [the system, systems component, or system service that the developer has access to is/are defined;]:

a. Has appropriate access authorizations as determined by assigned [official government duties assigned to the developer are defined;] ; and

b. Satisfies the following additional personnel screening criteria: [additional personnel screening criteria for the developer are defined;].

|  |
| --- |
| **SA-21 Control Summary Information** |
| Responsible Roles: Personnel Screening |
| Parameter sa-21\_odp.01: organization-defined information system, system component, or information system service |
| Parameter sa-21\_odp.02: organization-defined official government duties |
| Parameter sa-21\_odp.03: organization-defined additional personnel screening criteria |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SA-21 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  The customer is responsible for having appropriate access authorizations as determined by assigned organization-defined official government duties.  **Azure**  The Microsoft Security department conducts background checks and enforces the screening policies for all personnel. Background checks in the form of the Microsoft Cloud Screen are required for new hires or personnel transferring to positions that involve access to customers’ work sites and/or sensitive areas, including access to customer PII.  The Microsoft Cloud Screen includes the following:  \* Employment history check for the previous five years  \* Education Check (highest degree obtained)  \* Social Security Number (SSN) Check  \* Criminal History Check for the previous seven years  \* Office of Foreign Assets Control List (OFAC) Check  \* Bureau of Industry and Security List (BIS) Check  \* Office of Defense Trade Controls Debarred Persons List Check  Vendor staff with access to customer data are required to sign a background screening addendum with Microsoft or provide the results of the background screening from the third-party provider. Microsoft managers are required to include screening verbiage in their respective SOWs with vendors. |
| **Part B**  **Customer Responsibility**  The customer is responsible for satisfying organization-defined additional personnel screening criteria.  **Azure**  The Microsoft Security department conducts background checks and enforces the screening policies for all personnel. Background checks in the form of the Microsoft Cloud Screen are required for new hires or personnel transferring to positions that involve access to customers’ work sites and/or sensitive areas, including access to customer PII.  The Microsoft Cloud Screen includes the following:  \* Employment history check for the previous five years  \* Education Check (highest degree obtained)  \* Social Security Number (SSN) Check  \* Criminal History Check for the previous seven years  \* Office of Foreign Assets Control List (OFAC) Check  \* Bureau of Industry and Security List (BIS) Check  \* Office of Defense Trade Controls Debarred Persons List Check  Vendor staff with access to customer data are required to sign a background screening addendum with Microsoft or provide the results of the background screening from the third-party provider. Microsoft managers are required to include screening verbiage in their respective SOWs with vendors. |

## SA-22 Unsupported System Components

a. Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer; or

b. Provide the following options for alternative sources for continued support for unsupported components [Selection (OneOrMore): in-house support;[support from external providers is defined (if selected);] ] .

|  |
| --- |
| **SA-22 Control Summary Information** |
| Responsible Roles: Scanning |
| Parameter sa-22\_odp.01: organization-defined support from external providers |
| Parameter sa-22\_odp.02: |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SA-22 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  The customer is responsible for replacing information system components when support for the components is no longer available from the developer, vendor, or manufacturer.  **Azure**  Azure does not rely on components that are end of life or no longer supported. Azure tracks software and hardware end-of-life and end-of-support and establishes decommissioning plans as necessary. Azure tracks decommissioning of servers and network devices using dashboards and maintenance tickets. If necessary, Azure utilizes extended support from external vendors where available. |
| **Part B**  **Customer Responsibility**  The customer is responsible for providing options for alternative resources for the continued use of unsupported system components.  **Azure**  Azure does not rely on components that are end of life or no longer supported. Azure tracks software and hardware end-of-life and end-of-support and establishes decommissioning plans as necessary. Azure tracks decommissioning of servers and network devices using dashboards and maintenance tickets. If necessary, Azure utilizes extended support from external vendors where available. |

# System and Communications Protection (SC)

## SC-1 Policy and Procedures

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (OneOrMore): organization-level;mission/business-process-level;system-level] system and communications protection policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the system and communications protection policy and the associated system and communications protection controls;

b. Designate an [an official to manage the system and communications protection policy and procedures is defined;] to manage the development, documentation, and dissemination of the system and communications protection policy and procedures; and

c. Review and update the current system and communications protection:

1. Policy [at least annually] and following [events that would require the current system and communications protection policy to be reviewed and updated are defined;] ; and

2. Procedures [at least annually] and following [significant changes].

|  |
| --- |
| **SC-1 Control Summary Information** |
| Responsible Roles: SOP Team, Policy |
| Parameter sc-1(a): all personnel |
| Parameter sc-01\_odp.01: |
| Parameter sc-01\_odp.02: |
| Parameter sc-01\_odp.03: a Microsoft-wide |
| Parameter sc-01\_odp.04: the Microsoft Information Risk Management Council (IRMC) organization |
| Parameter sc-01\_odp.05: at least annually |
| Parameter sc-01\_odp.06: significant changes |
| Parameter sc-01\_odp.07: at least annually |
| Parameter sc-01\_odp.08: significant changes |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☒ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SC-1 What is the solution and how is it implemented?** |
| **Part A1**  **Customer Responsibility**  The customer is responsible for developing, documenting, and disseminating system and communications protection policy and procedures that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.  **Azure**  Azure addresses the Microsoft-level system and communications policies as part of the Microsoft security policies, of which there are two sets: the Microsoft Security Policy (MSP) that is applicable to all Microsoft personnel, and the Microsoft Security Program Policy (MSPP), which is applicable to all Microsoft personnel that have a responsibility for security. The Microsoft Information Risk Management Council (IRMC) is the governance body with review and approval responsibility for the MSP and MSPP. Within Azure, the MSPP specifically applies to all Microsoft personnel with security objectives such as designing, building, and operating Azure and across all information and processes used in the conduct of Microsoft business. All Azure personnel are accountable and responsible for complying with these guiding principles within their designated roles. The policies address the following:  \* Communications security  \* Communications across networks  \* Secure communications channels  \* Network design  Additionally, the policies address the purpose, scope, roles, responsibilities, compliance requirements, and required coordination among the various Microsoft organizations that provide levels of support to all services. The policies indicate Microsoft management’s commitment and are a critical component of the Microsoft risk management strategy, providing Azure personnel with a current set of clear and concise information security requirements. These policies are consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines currently applicable to Microsoft and Azure.  Service teams may supplement the Microsoft and Azure policies and procedures with service-specific policies and procedures. Service-specific policies and procedures associated with system and communications are documented and stored within internal service team SharePoint sites. Only personnel with authorized credentials, adequate levels of permission, legitimate need to know, and specific roles and responsibilities are given access to the service-specific policies or procedures. |
| **Part A2**  **Customer Responsibility**  The customer is responsible for procedures to facilitate the implementation of the system and communications protection policy and the associated system and communications protection controls.  **Azure**  C+AI Security publishes additional standard operating procedures (SOPs) and Security Standards that facilitate and support the implementation of systems and communications protection controls in Azure. These SOPs and standards include:  \* Azure Access Control Standard Operating Procedure (SOP)  \* Azure Asset Management Standard Operating Procedure (SOP)  \* Azure Cryptographic Control Standard Operating Procedure (SOP)  \* Key Management Standard  \* Asset Classification Standard  \* Asset Protection Standard  Service teams may supplement the Microsoft and Azure policies and procedures with service-specific policies and procedures. Service-specific policies and procedures associated with system and communications are documented and stored within internal service team SharePoint sites. Only personnel with authorized credentials, adequate levels of permission, legitimate need to know, and specific roles and responsibilities are given access to the service-specific policies or procedures. |
| **Part B**  **Customer Responsibility**  The customer is responsible for designating an official to manage the development, documentation, and dissemination of system and communications protection policy and procedures.  **Azure**  The Microsoft Information Risk Management Council (IRMC) organization is the governance body with approval responsibility for the Microsoft Security Policy (MSP) and Microsoft Security Program Policy (MSPP). The IRMC consists of representatives from security and risk management teams across Microsoft including Core Services Engineering and Operations (CSEO), Azure, and Global Security. The Customer Security and Trust: Security Engineering (CST-SE) organization manages the review and approval process and maintains the policies.  On an annual basis, the CST-SE conducts a line-by-line review of the MSP and MSPP. The Microsoft Security Policy (MSP) and Microsoft Security Program Policy (MSPP) Governance document describes each member’s role, types and frequency of review, escalation paths, approval process, and formal publishing procedures of the security policy. Throughout the year, if necessary, CST-SE may convene with the IRMC to conduct reviews after a significant review or change request. The approved policy update is published within the relevant tool on the Microsoft intranet. If service teams establish service-specific or team-specific policies, the respective service teams update the necessary policies at least annually. |
| **Part C1**  **Customer Responsibility**  The customer is responsible for reviewing and updating the current system and communications policy on a regular basis and following organization defined events.  **Azure**  The Azure team updates the Azure SOPs at least annually through a formal review process. If needed, the Azure team updates the SOP after a significant change affecting policy execution as well. If established, service-team-specific procedures are updated by their respective teams. The individual service teams review and update their respective SOPs at least annually and when required by a significant change. |
| **Part C2**  **Customer Responsibility**  The customer is responsible for reviewing and updating the current system and communications procedures on a regular basis and following organization defined events.  **Azure**  The Azure team updates the Azure SOPs at least annually through a formal review process. If needed, the Azure team updates the SOP after a significant change affecting policy execution as well. If established, service-team-specific procedures are updated by their respective teams. The individual service teams review and update their respective SOPs at least annually and when required by a significant change. |

## SC-2 Separation of System and User Functionality

Separate user functionality, including user interface services, from system management functionality.

|  |
| --- |
| **SC-2 Control Summary Information** |
| Responsible Roles: JIT |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SC-2 What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for separating user functionality, including user interface services, from system management functionality.  **Azure**  Azure separates functionality into standard access and elevated or privileged access, corresponding to user and system management functionality and ensuring logical separation of roles. All personnel with standard access are granted system metadata read access used for regular troubleshooting, release management, and other maintenance and monitoring activities. Standard access provides permissions to key Azure tools, services, SharePoint sites, documentation, and a variety of dashboards used to maintain the cloud, but does not permit any management functionality within the Azure cloud.  All personnel must use the Just in Time service (JIT) when elevated access is required in the Azure production environment. There is no standing or persistent elevated access to the Azure production environment. The primary exception is Break-Glass elevated access, utilized when the JIT service is unavailable, and described in detail in AC-02.  Azure further enforces logical separation by requiring the use of a Secure Admin Workstation (SAW) to access the Azure production environment and by limiting access to those SAWs only to specific users. The SAW is a locked-down Microsoft workstation which has minimal software installed. |

## SC-3 Security Function Isolation

Isolate security functions from nonsecurity functions.

|  |
| --- |
| **SC-3 Control Summary Information** |
| Responsible Roles: JIT |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SC-3 What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for isolating security functions from non-security functions for customer-deployed resources.  **Azure**  All Azure assets run modern operating systems as identified in the Azure inventory. These operating systems maintain separate execution domains for each executing process by assigning a private virtual address space to each process. See the following for more information:  <https://docs.microsoft.com/en-us/windows/win32/memory/memory-protection>  All Azure servers use either Intel or AMD processors. Both processor types implement isolation by means of protection rings with various privilege levels. User code runs in ring 3, while kernel code runs in ring 0.  Security software on the servers, such as antivirus and anti-malware software, is protected using access control lists at the file system level via file permissions. This ensures that only approved users have access to security software. These are technological implementations and are in place continuously.  At the network level, Azure implements Jumpboxes, Debug Servers, Hop Boxes, and a VPN to restrict access to security functions. To access security functions, users must first log on to the Jumpboxes, Debug Servers, Hop Boxes, or VPN using multifactor authentication. Azure monitors and audits access using the logging and monitoring pipeline. Azure users must also use JIT to access production assets. In this way, Azure restricts access to security functions by implementing least privilege capabilities throughout the environment. |

## SC-4 Information in Shared System Resources

Prevent unauthorized and unintended information transfer via shared system resources.

|  |
| --- |
| **SC-4 Control Summary Information** |
| Responsible Roles: Networking, Compute |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SC-4 What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for preventing unauthorized and unintended information transfer between customer-deployed resources.  **Azure**  In order to transfer residual information on an Azure asset, the user must first access the asset. Azure prevents unauthorized and unintended information transfer by implementing several technical controls within the network, including isolation via VLANs and Network Security Groups (NSGs), and implementing strict flow control via ACLs to Azure from other internal Microsoft networks and from the internet. Strong access controls including multifactor authentication, JIT, and usage of security groups limit any unauthorized or unintended transfer of information through shared resources at an access control level. Azure performs logging and monitoring on all assets as a detective measure as well.  Azure follows strict standards for overwriting storage resources before their reuse or the physical destruction of decommissioned hardware. Azure executes a complete deletion of data on customer request and on contract termination.  Protection of Virtual Machines (VMs) is provided by hypervisor isolation of the Root OS from the Guest OS and the Guest OS from one another. The hypervisor acts like a micro-kernel and passes all hardware access requests from the Guest OS to the Root OS for processing using a shared-memory interface. This prevents users from obtaining raw read/write/execute access to the system and mitigates the risk of sharing system resources. On each node, the Azure Hypervisor runs directly over the hardware and divides a node into a variable number of Guest VMs running the Guest OS. Each node also has one VM with administrative privileges which runs the Host OS. The Host OS is given more priority than any guest VM to prevent a guest VM delaying or interfering with Host OS processes. The Host OS hosts a Fabric Agent (FA) that communicates with the Fabric Controller (FC). FAs are used in turn to manage guest agents (GA) within Guest OSes on customer VMs. The FCs manage Azure operating system resources and monitors the tenants for resource usage ensuring that tenants that are of high impact are moved to a source that has more capacity availability if needed. The FCs move tenants around to support resource consumption as part of the unique Azure functionality. Each FC manages the lifecycle of applications running in its cluster and provisions and monitors the health of the hardware under its control. It runs autonomic operations, such as reincarnating VM instances on healthy servers when it determines that a server has failed. At the Guest VM, Windows Firewall is enabled on each Guest VM and the only ports open and addressable internally or externally are those explicitly defined in the Service Definition file configured by the customer. All traffic and access to disks and networks is mediated by the Azure Hypervisor and Host OS. Azure also runs the Native OS, a customized OS that runs on nodes that do not have a hypervisor. The FC controls the full OS as if it were a VM. Certain Azure internal services run on the Native OS alone – nodes deployed by the service teams that have no corresponding VMs. Azure also utilizes certain servers that operate as Bare Metal servers, which is like the Native OS but is not managed by the Fabric Controller as if it were a VM. Bare Metal servers are fully provisioned physical nodes. |

## SC-5 Denial-of-service Protection

a. [Selection: protect against;limit] the effects of the following types of denial-of-service events: [at a minimum: ICMP (ping) flood, SYN flood, slowloris, buffer overflow attack, and volume attack] ; and

b. Employ the following controls to achieve the denial-of-service objective: [controls to achieve the denial-of-service objective by type of denial-of-service event are defined;].

|  |
| --- |
| **SC-5 Control Summary Information** |
| Responsible Roles: Networking, Compute, Storage, SQL DB |
| Parameter sc-05\_odp.01: attacks on bandwidth, transactional capacity, and storage |
| Parameter sc-05\_odp.02: Protect against |
| Parameter sc-05\_odp.03: geo-replication, IP address blocking, network-based DDoS protections |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SC-5 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for protecting customer-deployed resources from denial of service (DOS) attacks.  **Azure**  Azure has implemented protection mechanisms as described in Part b below to protect against three kinds of DoS attacks: attacks on bandwidth, attacks on transactional capacity (authentication overhead, IOPS, cache efficiency, etc.), and attacks on storage capacity. |
| **Part B**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for protecting customer-deployed resources from denial of service (DOS) attacks.  **Azure**  Azure uses A10 distributed denial of service (DDoS) protection network devices that provide automated detection and mitigation. The DDoS protection solution utilizes Azure Network Monitoring (NetMon) to sample network flow packets and determine if there is an attack. Once the attack is detected, the A10s are used as scrubbers to mitigate attacks. After mitigation, further clean traffic is allowed into the Azure environment. This involves the NetMon and Geneva Monitoring features to detect attacks and use A10 technology to mitigate attacks. This solution is designed to withstand attacks from both outside and inside of Azure. For attacks initiated within Azure to another Azure tenant, trusted IP filters prevent spoofing of dynamic IP (DIP) address. Azure monitors and isolates or removes offending VMs from the network.  Additional DoS protection solutions include:  \* UDP IPv4 and IPv6 flood protection  \* ICMP IPv4 and IPv6 flood protection  \* TCP IPv4 and IPv6 flood protection  \* TCP SYN attack protection for IPv4 and IPv6  \* Fragmentation attack protection  **Azure Storage**  Azure has implemented protection mechanisms as defined below to protect from DoS attacks on Azure Storage: attacks on bandwidth, attacks on transactional capacity (ICMP (ping) flood, SYN flood, slowloris, buffer overflow attack, and volume attack, etc.), and attacks on storage capacity.  Attacks on bandwidth are handled by identifying the IP addresses of assets mounting simple attacks and blocking them as early in the communications stream as possible. The ability to throttle or disable abusive accounts is provided.  Storage accounts that suddenly start growing out of proportion to past patterns may represent a DoS attack against a customer or more likely represent a bug in a customer program. This is tracked by actively monitoring bandwidth, transactions, and storage capacity usage and growth by storage account and IP address across the whole storage stamp. If the metrics start to change in an unexpected way, Azure analyzes storage accounts and IP addresses and performs a range of mitigations. This ranges from throttling the accounts or IPs, contacting the customers, or even disabling or putting the accounts or IPs into read-only mode.  In addition to dealing with abusive storage accounts and IP address ranges in the above manner, Azure Storage monitors the (a) bandwidth, (b) transactions, and (c) storage capacity for each of the stamps. If any of these metrics reach seventy (70) percent of peak capacity provided by the storage stamp, then Azure Storage load-balances storage accounts via geo-replication migration across the storage stamps preferably within a given geo-location to keep the capacity below this threshold for each production storage stamp.  **Azure SQL DB**  Azure has implemented protection mechanisms as defined below to protect from DoS attacks on Azure SQL DB (ICMP (ping) flood, SYN flood, slowloris, buffer overflow attack, and volume attack, etc.). Azure SQL DB gateway performs stateful TDS packet inspection while accepting connections from clients to validate the connection information and pass on the TDS packets to the appropriate server based on the database name specified in the connection string. In the back-end, Azure SQL databases are hosted in tenant rings that are deployed in Virtual Networks (VNets). The OneDDOS system protects traffic coming into these VNets. They define normal thresholds on each endpoint, and if the thresholds are exceeded, they route the traffic through A10 devices which scrub the traffic to prevent DOS attacks.  Additionally, Azure SQL Database offers a variety of network access controls so customers can choose between public or private connectivity. Customers can use a combination of these network access controls to control how clients can connect to SQL Database and thus reduce the surface area for DoS attacks. Public connections are blocked by SQL DB firewall and traffic is allowed only when the client IP addresses is added in the form of a firewall rule. Access from resources inside Azure, such as an Azure VM or Web App, can be accomplished by using Service Endpoints and VNet firewall rules. Lastly customers can use private endpoint such that Azure SQL DB is associated with a specific private IP address within a specific VNet and subnet. |

## SC-7 Boundary Protection

a. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system;

b. Implement subnetworks for publicly accessible system components that are [Selection: physically;logically] separated from internal organizational networks; and

c. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.

(b) Guidance: SC-7 (b) should be met by subnet isolation. A subnetwork (subnet) is a physically or logically segmented section of a larger network defined at TCP/IP Layer 3, to both minimize traffic and, important for a FedRAMP Authorization, add a crucial layer of network isolation. Subnets are distinct from VLANs (Layer 2), security groups, and VPCs and are specifically required to satisfy SC-7 part b and other controls. See the FedRAMP Subnets White Paper (https://www.fedramp.gov/assets/resources/documents/FedRAMP\_subnets\_white\_paper.pdf) for additional information.

|  |
| --- |
| **SC-7 Control Summary Information** |
| Responsible Roles: Logging and Monitoring, Networking, VPN, Jumpbox |
| Parameter sc-7(b): physically and logically |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SC-7 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for monitoring and controlling communications at and within the managed interfaces of the customer-deployed system.  **Azure**  Azure implements boundary protection through a defense-in-depth strategy. As a cloud service comprised of numerous service teams and customers, logical isolation and segmentation are critical to the secure operations of Azure. The strategy includes network segmentation through VLAN and Network Security Group (NSG) segmentation, ACL restrictions, and encrypted communications.  Internally, at the network level, Azure implements Jumpboxes, Debug Servers, Hop Boxes, and a VPN to restrict access to the Azure environment. To access the environment, users must first log on to the Jumpboxes, Debug Servers, Hop Boxes, or VPN using multifactor authentication.  Azure is logically segmented into the management plane, which is heavily restricted to only key service teams necessary to administer underlying networking and foundational services, and the customer plane, upon which all Azure service teams and external customers reside and operate. Internal Azure service teams utilize the same logical isolation techniques that customers use to ensure their deployments are secure. Microsoft utilizes the Azure Security Pack (AzSecPack) service for log generation, consolidation, and monitoring throughout the Azure cloud.  The logical isolation of internal and customer infrastructure in a hyperscale cloud is fundamental to maintaining security. The overarching principle for a virtualized solution is to allow only connections and communications that are necessary for that virtualized solution to operate, blocking all other ports and connections by default. Azure Virtual Networks (VNets) ensure that all private network traffic is logically isolated from traffic belonging to other internal and external networks. Virtual Machines (VMs) in one VNet cannot communicate directly with VMs in a different VNet even if both VNets are created by the same user. Networking isolation ensures that communication between VMs remains private within a VNet.  VNets provide isolation of network traffic between tenants as part of their fundamental design. A subscription can contain multiple logically isolated private networks, and include firewall, load balancing, and network address translation. Each VNet is isolated from other VNets by default. Multiple deployments inside the same subscription can be placed on the same VNet, and then communicate with each other through private IP addresses.  Network access to VMs is limited by packet filtering at the network edge, at load balancers, and at the Host OS level. Each service team additionally configures their host firewalls to further limit connectivity, specifying for each listening port whether connections are accepted from the external networks or only from role instances within the same cloud service or VNet.  Azure provides network isolation for each deployment and enforces the following rules:  \* Traffic between VMs always traverses through trusted packet filters.  \* Protocols such as Address Resolution Protocol (ARP), Dynamic Host Configuration Protocol (DHCP), and other OSI Layer-2 traffic from a VM are controlled using rate-limiting and anti-spoofing protection.  \* VMs cannot capture any traffic on the network that is not intended for them.  \* VMs cannot send traffic to Azure private interfaces and infrastructure services, or to other user's VMs. VMs can only communicate with other VMs owned or controlled by the same team and with Azure service endpoints.  \* When users put VMs on a VNet, those VMs get their own address spaces that are invisible, and hence, not reachable from VMs outside of a deployment or virtual network (unless configured to be visible via IP addresses). These environments are open only through the ports that users specify for access; if the VM is defined to have an external IP address, then all ports are open for external access.  Local connections are disallowed by policy within Azure. No personnel have local access. Azure performs network monitoring and detection of unauthorized connections via Network Isolation (NetIso), which provides the Network Risk Management Service (NRMS) for network baseline measurement, management, and enforcement. The service provides an assessment of network security and alerts on internet-exposed endpoints via Incident Management (IcM) based on analysis patterns for configuration issues. Any process that begins offering an open network port is flagged and investigated if it is not part of the approved baseline for that host to ensure detection of network services that have not been authorized as an indicator of compromise. In addition, the implemented host-based SDN firewall uses a deny all policy.  Azure’s hyperscale network is designed to provide uniform high capacity between servers, performance isolation between services, and Ethernet Layer-2 semantics. Azure uses a number of networking implementations to achieve these goals: flat addressing to allow service instances to be placed anywhere in the network; load balancing to spread traffic uniformly across network paths; and end-system based address resolution to scale to large server pools, without introducing complexity to the network control plane.  These implementations give each service the illusion that all the servers assigned to it, and only those servers, are connected by a single non-interfering Ethernet switch – a Virtual Layer 2 (VL2) – and maintain this illusion even as the size of each service varies from one server to hundreds of thousands. This VL2 implementation achieves traffic performance isolation, ensuring that it is not possible that the traffic of one service could be affected by the traffic of any other service, as if each service were connected by a separate physical switch.  The Azure network uses two different IP-address families:  \* The customer address (CA) is the defined/chosen VNet IP address, also referred to as Virtual IP (VIP). The network infrastructure operates using CAs, which are externally routable. All switches and interfaces are assigned CAs, and switches run an IP-based (Layer-3) link-state routing protocol that disseminates only these CAs. This design allows switches to obtain the complete switch-level topology, as well as forward packets encapsulated with CAs along shortest paths.  \* The provider address (PA) is the Azure-assigned internal Fabric address that is not visible to users and is also referred to as Dynamic IP (DIP). No traffic goes directly from the external network to an asset; all traffic from external networks must go through a Software Load Balancer (SLB) and be encapsulated to protect the internal Azure address space by only routing packets to valid Azure internal IP addresses and ports. Network Address Translation (NAT) separates internal network traffic from external traffic. Internal traffic uses RFC 1918 address space or private address space – the provider addresses (PAs) – that is not externally routable. The translation from the PA to the CA is performed at the SLBs. CAs - that are externally routable - are translated into internal provider addresses (PAs) that are only routable within Azure. These addresses remain unaltered no matter how their servers’ locations change due to virtual-machine migration or reprovisioning.  Each PA is associated with a CA, which is the identifier of the Top of Rack (ToR) switch to which the server is connected. VL2 uses a scalable, reliable directory system to store and maintain the mapping of PAs to CAs, and this mapping is created when servers are provisioned to a service and assigned PA addresses. An agent running in the network stack on every server, called the VL2 agent, invokes the directory system’s resolution service to learn the actual location of the destination and then tunnels the original packet there.  Azure assigns servers IP addresses that act as names alone, with no topological significance. Azure’s VL2 addressing scheme separates these server names (PAs) from their locations (CAs). The crux of offering Layer-2 semantics is having servers believe they share a single large IP subnet – i.e., the entire PA space – with other servers in the same service, while eliminating the Address Resolution Protocol (ARP) and Dynamic Host Configuration Protocol (DHCP) scaling bottlenecks that plague large Ethernet deployments.  A server cannot send packets to a PA if the directory service refuses to provide it with a CA through which it can route its packets, which means that the directory service enforces access control policies. Further, since the directory system knows which server is making the request when handling a lookup, it can enforce fine-grained isolation policies. For example, it could enforce the policy that only servers belonging to the same service can communicate with each other.  To route traffic between servers, which use PA addresses, on an underlying network that knows routes for CA addresses, the VL2 agent on each server captures packets from the host, and encapsulates them with the CA address of the ToR switch of the destination. Once the packet arrives at the CA (i.e., the destination ToR switch), the destination ToR switch decapsulates the packet and delivers it to the destination PA carried in the inner header. The packet is first delivered to one of the Intermediate switches, decapsulated by the switch, delivered to the ToR’s CA, decapsulated again, and finally sent to the destination.  For external traffic, Azure provides multiple layers of assurance to enforce isolation depending on traffic patterns. When a user places an external IP on their VNet gateway, traffic from the external network that is destined for that IP address will be routed to an Edge Router. Azure then uses Border Gateway Protocol (BGP) to share routing details with the external network to establish end-to-end connectivity. When communication begins with a resource within the VNet, the network traffic traverses as normal until it reaches a Microsoft ExpressRoute Edge (MSEE) Router. In both cases, VNets provide the means for Azure VMs to act as part of the user's external network. A cryptographically protected IPsec/IKE tunnel is established between Azure and user's internal network (e.g., via Azure VPN Gateway or Azure ExpressRoute Private Peering), enabling the VM to connect securely to the user's resources as though it was directly on that network.  At the Edge Router or the MSEE Router, the packet is encapsulated using Generic Routing Encapsulation (GRE). This encapsulation uses a unique identifier specific to the VNet destination and the destination address, which is used to appropriately route the traffic to the identified VNet. Upon reaching the VNet Gateway, which is a special VNet used only to accept traffic from outside of an Azure VNet, the encapsulation is verified by the Azure network fabric to ensure:  \* the endpoint receiving the packet is a match to the unique VNet ID used to route the data, and  \* the destination address requested exists in this VNet.  Once verified, the packet is routed as internal traffic from the VNet Gateway to the final requested destination address within the VNet. This approach ensures that traffic from external networks travels only to the Azure VNet for which it is destined, enforcing isolation.  Internal traffic also uses GRE encapsulation/tunneling. When two resources in an Azure VNet attempt to establish communications between each other, the Azure network fabric reaches out to the Azure VNet routing directory service that is part of the Azure network fabric. The directory services use the customer address (CA) and the requested destination address to determine the provider address (PA). This information, including the VNet identifier, CA, and PA, is then used to encapsulate the traffic with GRE. The Azure network uses this information to properly route the encapsulated data to the appropriate Azure host using the PA. The encapsulation is reviewed by the Azure network fabric to confirm:  \* the PA is a match,  \* the CA is located at this PA, and  \* the VNet identifier is a match.  Once all three are verified, the encapsulation is removed and routed to the CA as normal traffic (e.g., to a VM endpoint). This approach provides VNet isolation assurance based on correct traffic routing between cloud services.  Azure VNets implement several mechanisms to ensure secure traffic between tenants. These mechanisms align to existing industry standards and security practices, and prevent well-known attack vectors including:  \* Prevent IP address spoofing – Whenever encapsulated traffic is transmitted by a VNet, the service reverifies the information on the receiving end of the transmission. The traffic is looked up and encapsulated independently at the start of the transmission, as well as reverified at the receiving endpoint to ensure the transmission was performed appropriately. This verification is done with an internal VNet feature called SpoofGuard, which verifies that the source and destination are valid and allowed to communicate, thereby preventing mismatches in expected encapsulation patterns that might otherwise permit spoofing. The GRE encapsulation processes prevent spoofing as any GRE encapsulation and encryption not done by the Azure network fabric is treated as dropped traffic.  \* Provide network segmentation across service teams with overlapping network spaces – Azure VNet’s implementation relies on established tunneling standards such as the GRE, which in turn allows the use of specific unique identifiers (VNet IDs) throughout the cloud. The VNet identifiers are used as scoping identifiers. This approach ensures that a service team is always operating within their unique address space, overlapping address spaces between tenants, and the Azure network fabric. Anything that has not been encapsulated with a valid VNet ID is blocked within the Azure network fabric. In the example described above, any encapsulated traffic not performed by the Azure network fabric is discarded.  \* Prevent traffic from crossing between VNets – Preventing traffic from crossing between VNets is done through the same mechanisms that handle address overlap and prevent spoofing. Traffic crossing between VNets is rendered infeasible by using unique VNet IDs established per tenant in combination with verification of all traffic at the source and destination. Users do not have access to the underlying transmission mechanisms that rely on these IDs to perform the encapsulation. Consequently, any attempt to encapsulate and simulate these mechanisms would lead to dropped traffic.  In addition to these key protections, all unexpected traffic originating from external networks is dropped by default. Any packet entering the Azure network will first encounter an Edge router. Edge routers intentionally allow all inbound traffic into the Azure network except spoofed traffic. This basic traffic filtering protects the Azure network from known bad malicious traffic. Azure also implements DDoS protection at the network layer, collecting logs to throttle or block traffic based on real time and historical data analysis, and mitigates attacks on demand.  Moreover, the Azure network fabric blocks traffic from any IPs originating in the Azure network fabric space that are spoofed. The Azure network fabric uses GRE and Virtual Extensible LAN (VXLAN) to validate that all allowed traffic is Azure-controlled traffic and all non-Azure GRE traffic is blocked. By using GRE tunnels and VXLAN to segment traffic using unique keys, Azure meets RFC 3809 and RFC 4110. When using Azure VPN Gateway in combination with ExpressRoute, Azure meets RFC 4111 and RFC 4364. With a comprehensive approach for isolation encompassing external and internal network traffic, Azure VNets provide customer with assurance that Azure successfully routes traffic between VNets, allows proper network segmentation for tenants with overlapping address spaces, and prevents IP address spoofing.  Service teams are also able to utilize Azure services to further isolate and protect their resources. Using Network Security Groups (NSGs), a feature of Azure Virtual Network, service teams can filter traffic by source and destination IP address, port, and protocol via multiple inbound and outbound security rules – essentially acting as a distributed virtual firewall and IP-based network Access Control List (ACL). Service teams can apply an NSG to each NIC in a Virtual Machine, apply an NSG to the subnet that a NIC, or another Azure resource, is connected to, and directly to Virtual Machine Scale Sets, allowing finer control over the service team infrastructure.  At the infrastructure layer, Azure implements a Hypervisor firewall to protect all tenants running on top of the Hypervisor within virtual machines from unauthorized access. This Hypervisor firewall is distributed as part of the NSG rules deployed to the Host, implemented in the Hypervisor, and configured by the Fabric Controller agent. The Host OS instances utilize the built-in Windows Firewall to implement fine-grained ACLs at a greater granularity than router ACLs and are maintained by the same software that provisions tenants, so they are never out of date. They are applied using the Machine Configuration File (MCF) to Windows Firewall.  At the top of the operating system stack is the Guest OS, which service teams utilize as their operating system. By default, this layer does not allow any inbound communication to cloud service or virtual network, essentially making it part of a private network. |
| **Part B**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for implementing subnetworks for customer-deployed resources to logically separate publicly accessible resources from internal resources.  **Azure**  The only externally accessible components of Azure are the load balancers and the externally-facing server roles. All non-externally accessible Azure components connect to the load balancers via physically separate network interfaces on subnets that are logically separated from internal subnets. The hypervisor is isolated from interactions by virtual machines on port 80.  Azure employs Remote Desktop Protocol (RDP)and SSL VPN as the internal/external managed interface for interactive access to the Azure environment. Azure requires encrypted connections for connectivity from any of the solutions used to access the environment in accordance with Microsoft security architecture requirements. |
| **Part C**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for restricting connections to external networks or systems through managed interfaces, consisting of boundary protection devices arranged in accordance with the customer's security and privacy architecture.  **Azure**  Azure connects to external networks or information systems only through Azure Networking’s managed networks and Edge Routers. The network interfaces provide boundary protection at the Edge Router network level and are arranged in accordance with the Microsoft and Azure security architectures. Additional measures in place to help protect Azure information systems from malicious activities include:  \* Software load balancers  \* Non-routable IP addressing  \* Packet filtering  \* Host-based firewalls  \* VLAN and NSG isolation  \* Jumpboxes, Debug Servers, Hop Boxes, and VPNs  All traffic at the boundary is restricted to authorized connections as defined by the service team. |

### SC-7(3) - Access Points

Limit the number of external network connections to the system.

|  |
| --- |
| **SC-7(3) Control Summary Information** |
| Responsible Roles: Networking, Jumpbox |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SC-7(3) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for limiting the number of external connections established to the customer-deployed system.  **Azure**  Azure controls and monitors all inbound and outbound traffic through a limited number of network access points at the boundary and at key points within Azure. Azure leverages the following security mechanisms to limit the number of external network connections:  \* Load balancing and limiting inbound access to Azure, Azure Management Portal, front-end, and customer VM RDP. Each datacenter contains two groups of Jumpboxes, Debug Servers, and Hop Boxes behind a load balancer to limit the access points for Azure internal traffic, and customer traffic passes through a load balancer as well. Both entry points are monitored and generate audit logs and alerts in near-real time.  \* Jumpboxes , Debug servers, and Network Hop Boxes control all access to Azure.  \* Azure services are only accessible to customer users through the Azure provisioning portal and Web Services (REST API) interfaces. |

### SC-7(4) - External Telecommunications Services

(a) Implement a managed interface for each external telecommunication service;

(b) Establish a traffic flow policy for each managed interface;

(c) Protect the confidentiality and integrity of the information being transmitted across each interface;

(d) Document each exception to the traffic flow policy with a supporting mission or business need and duration of that need;

(e) Review exceptions to the traffic flow policy [at least every ninety (90) days or whenever there is a change in the threat environment that warrants a review of the exceptions] and remove exceptions that are no longer supported by an explicit mission or business need;

(f) Prevent unauthorized exchange of control plane traffic with external networks;

(g) Publish information to enable remote networks to detect unauthorized control plane traffic from internal networks; and

(h) Filter unauthorized control plane traffic from external networks.

|  |
| --- |
| **SC-7(4) Control Summary Information** |
| Responsible Roles: Logging and Monitoring, Networking |
| Parameter sc-07.04\_odp: quarterly with traffic flow monitoring times per day |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SC-7(4) What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  The customer is responsible for implementing a managed interface for each external telecommunication service.  **Azure**  Network access to Azure is limited by packet filtering at the network edge, at load balancers, and at the Host OS level. Service teams additionally configure their host firewalls to further limit connectivity, specifying for each listening port whether connections are accepted from external networks or only from role instances within the same cloud service or VNet. |
| **Part B**  **Customer Responsibility**  The customer is responsible for establishing a traffic flow policy for each managed interface.  **Azure**  The Azure Networking team establishes routing policies and ACLs at the edge to only allow the export of 8075 public blocks to Azure's Border Gateway Protocol (BGP) peers. Edge Access Control Lists (ACLs) are applied inbound from all peering interfaces. The policy explicitly filters non-edge protocols such as SQL, RPC, 445, and 135-139 from entering the network from untrusted sources.  Service teams running on top of the fabric customize the routing policies and ACLs necessary for their service. For instance, the Azure Portal needs to be externally accessible, but the JIT Portal does not. |
| **Part C**  **Customer Responsibility**  The customer is responsible for protecting the confidentiality and integrity of the information being transmitted across each interface.  **Azure**  Azure requires the use of TLS 1.2/1.3 throughout the cloud. A TLS scanner hosted by Unified Remoting Scanning (URSA) is used to determine the status of Azure encryption in transit, specifically the use of TLS 1.2/1.3 or higher. |
| **Part D**  **Customer Responsibility**  The customer is responsible for documenting each exception to the traffic flow policy with a supporting mission/business need and duration of that need.  **Azure**  Azure documents exceptions to the traffic flow policy outside the standard, approved baseline via the security review process with a supporting mission/business need and duration of that need. In the event an exception is needed from the traffic flow policy, a security review is documented and reviewed by the C+AI Security team. |
| **Part E**  **Customer Responsibility**  The customer is responsible for reviewing exceptions to the traffic flow policy at an organization-defined frequency and removing exceptions that are no longer supported by an explicit mission/business need.  **Azure**  Azure reviews each change to the network ACL via the C+AI Security Policy Exception process with a supporting mission/business need and duration of that need. In the event an exception is needed, a security review (SR) is documented and reviewed by the C+AI Security team.  All exceptions are reviewed on at least a semiannual basis. The Azure Networking team removes all exceptions that are no longer supported by a business need in Azure. If the Azure Networking team identifies and reviews a policy exception that is no longer needed, they remove that exception.  At the infrastructure level, Azure blocks administrative ports on the internet edge of the environment through the Edge ACL baseline. To detect any authorized changes to the established traffic flow polices on the Azure boundary the Azure Security Monitoring (ASM) team automatically scans the internet boundary of the Azure environment every four (4) hours. If a blocked port is opened, a ticket is automatically created in the ticketing system and an alert is created for the Azure Security Response Team to remediate. |
| **Part F**  **Customer Responsibility**  The customer is responsible for preventing unauthorized exchange of control plane traffic with external networks.  **Azure**  As described in the Microsoft Security Program Policy (MSPP) and associated standards, Azure employs a deny-all, permit-by-exception policy for allowing the Azure information system to connect to external information systems. Currently, Azure does not have any connections to external information systems. The only interconnections are with internal Microsoft services. The internal Microsoft services that connect with Azure cloud are CorpNet and Cosmos. CorpNet is the Microsoft corporate network. CorpNet contains services run on Microsoft’s corporate network, not dedicated to Azure, such as source code repositories, system document repositories, and change ticketing. Cosmos is a service, not dedicated to Azure, that stores and reports on Azure log data. AAD scrubs logs of customer information before sending logs to Cosmos. Azure does not require ISAs/MOUs for connections internal to Microsoft. |
| **Part G**  **Customer Responsibility**  The customer is responsible for publishing information to enable remote networks to detect unauthorized control plane traffic from internal networks.  **Azure**  The overarching principle for a virtualized solution is to allow only connections and communications that are necessary for that virtualized solution to operate, blocking all other ports, protocols, and connections by default. Azure only allows connections and communication that are necessary to operate the system and only after being explicitly opened. Connections are managed at the system boundary using Azure Networking boundary protection devices. Connections within the boundary are managed using:  \* IP Filtering  \* Network Security Group (NSG) ACLs  \* VFP Filtering (for virtual machines)  \* Host-based firewalls  \* Guest firewalls (for virtual machines) |
| **Part H**  **Customer Responsibility**  The customer is responsible for filtering unauthorized control plane traffic from external networks.  **Azure**  Azure controls and monitors all inbound and outbound traffic through a limited number of network access points at the boundary and at key points within Azure. Azure leverages the following security mechanisms to limit the number of external network connections:  \* Load balancing and limiting inbound access to Azure, Azure Management Portal, front-end, and customer VM RDP. Each datacenter contains two groups of Jumpboxes, Debug Servers, and Hop Boxes behind a load balancer to limit the access points for Azure internal traffic, and customer traffic passes through a load balancer as well. Both entry points are monitored and generate audit logs and alerts in near-real time.  \* Jumpboxes , Debug servers, and Network Hop Boxes control all access to Azure.  \* Azure services are only accessible to customer users through the Azure provisioning portal and Web Services (REST API) interfaces. |

### SC-7(5) - Deny by Default - Allow by Exception

Deny network communications traffic by default and allow network communications traffic by exception [Selection (OneOrMore): at managed interfaces;for [systems for which network communications traffic is denied by default and network communications traffic is allowed by exception are defined (if selected).] ] .

Guidance: For JAB Authorization, CSPs shall include details of this control in their Architecture Briefing

|  |
| --- |
| **SC-7(5) Control Summary Information** |
| Responsible Roles: Networking |
| Parameter sc-07.05\_odp.01: any systems or Azure components |
| Parameter sc-07.05\_odp.02: |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SC-7(5) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for configuring managed network interfaces to deny all traffic by default and allow by exception.  **Azure**  The overarching principle for a virtualized solution is to allow only connections and communications that are necessary for that virtualized solution to operate, blocking all other ports, protocols, and connections by default. Azure only allows connections and communication that are necessary to operate the system and only after being explicitly opened. Connections are managed at the system boundary using Azure Networking boundary protection devices. Connections within the boundary are managed using:  \* IP Filtering  \* Network Security Group (NSG) ACLs  \* VFP Filtering (for virtual machines)  \* Host-based firewalls  \* Guest firewalls (for virtual machines)  As described in the Microsoft Security Program Policy (MSPP) and associated standards, Azure employs a deny-all, permit-by-exception policy for allowing the Azure information system to connect to external information systems. Currently, Azure does not have any connections to external information systems. The only interconnections are with internal Microsoft services. The internal Microsoft services that connect with Azure cloud are CorpNet and Cosmos. CorpNet is the Microsoft corporate network. CorpNet contains services run on Microsoft’s corporate network, not dedicated to Azure, such as source code repositories, system document repositories, and change ticketing. Cosmos is a service, not dedicated to Azure, that stores and reports on Azure log data. AAD scrubs logs of customer information before sending logs to Cosmos. Azure does not require ISAs/MOUs for connections internal to Microsoft. |

### SC-7(7) - Split Tunneling for Remote Devices

Prevent split tunneling for remote devices connecting to organizational systems unless the split tunnel is securely provisioned using [safeguards to securely provision split tunneling are defined;].

|  |
| --- |
| **SC-7(7) Control Summary Information** |
| Responsible Roles: VPN |
| Parameter sc-07.07\_odp: safeguards |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SC-7(7) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for preventing split tunneling for remote devices connecting to the customer-deployed system.  **Azure**  Azure sessions do not permit split tunneling. Azure utilizes an L4 VPN which does not allow split tunneling – this feature only works with L3 VPNs. All connections are made over Federal Information Processing Standards (FIPS) 140-2 TLS encrypted connections and authenticated using multifactor authentication (MFA). Azure does not permit remote devices to establish non-remote connections (such as VPNs) with the Azure environment. In order to access the Azure environment, a user must authenticate with their Azure domain credentials either through an Azure Remote Desktop Gateway boundary device via the Microsoft remote desktop connection client (internet accessible) or through a connection (not internet accessible). |

### SC-7(8) - Route Traffic to Authenticated Proxy Servers

Route [internal communications traffic to be routed to external networks is defined;] to [any network outside of organizational control and any network outside the authorization boundary] through authenticated proxy servers at managed interfaces.

|  |
| --- |
| **SC-7(8) Control Summary Information** |
| Responsible Roles: Networking |
| Parameter sc-07.08\_odp.01: internal management systems |
| Parameter sc-07.08\_odp.02: approved URLs |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☒ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☒ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SC-7(8) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for routing customer-defined information through an authenticated proxy to an external network.  **Azure**  This control does not apply to Azure. Proxy servers are not deployed in Azure since Azure does not externally route internal traffic. This control is related to controlling and monitoring client-initiated internet communications (e.g. outbound HTTP proxies). Clients/desktops are not in the scope of Azure and are managed by the customer. These connections to Azure assets are managed by Azure and are controlled by the Azure Networking team. |

### SC-7(10) - Prevent Exfiltration

(a) Prevent the exfiltration of information; and

(b) Conduct exfiltration tests [the frequency for conducting exfiltration tests is defined;].

|  |
| --- |
| **SC-7(10) Control Summary Information** |
| Responsible Roles: Logging and Monitoring, Networking |
| Parameter sc-07.10\_odp: organization-defined frequency |
| Implementation Status (check all that apply):  ☐ Implemented  ☒ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SC-7(10) What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for preventing unauthorized exfiltration of information across managed interfaces.  **Azure**  For Azure services, onboarding to Azure Security Pack (AzSecPack) enables monitoring of network communication correlated with network logs and in-memory lateral movement during post exploitation for all deployment types via Process Investigation, which is available externally via Microsoft Defender for Cloud via Fileless Attack detections, and via the Network Risk Management (NRM) Service. The NRM service assesses the resultant set of open ports and protocols based on data provided by the VM agent. Additionally, for VMs hosted on Azure, the Network Security Group (NSG) settings are considered and the resultant set of the settings is calculated. Additionally, for the assets running in Bare Metal, Azure assesses the Surface Area Manager configuration settings. For Linux VMs hosted in Azure, Azure uses the NSG settings to validate that the configuration meets the network baseline requirements. For all deployment types, if there is a network baseline violation that exposes a management port to the internet, an alert is generated and provided to the service team.  For internal services, there is monitoring and alerting for unusual behavior of key security features including, but not limited to, if a user accesses an asset without using Azure Just In Time (JIT) access, if a dSTS account has an unusual access pattern, if the Geneva Actions have unusual activity, if the Azure Fabric is accessed without using Azure JIT, or if a service owner has unexpected changes to permissions in the service team subscription.  Additionally, service teams regardless of deployment type must monitor their own network connections for unexpected network activities at the application layer. However, to protect customer end user identifiable information, Azure does not monitor the customer traffic in the security monitoring solutions.  Azure does not inspect or monitor customer traffic. By default, Microsoft is unaware of what data is outbound from the environment by the customer. In the event of customer data spillage, upon customer request, Microsoft may assist with the incident including accessing customer data according to the Azure Incident Management Standard Operating Procedure (SOP). |
| **Part B**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for conducting exfiltration tests at organization-defined frequency.  **Azure**  The Third Party Assessment Organization (3PAO) performs penetration testing on the information system at least annually which includes exfiltration testing. The Penetration Test Report covers Azure system components identified as part of the authorization boundary. |

### SC-7(12) - Host-based Protection

Implement [Host Intrusion Prevention System (HIPS), Host Intrusion Detection System (HIDS), or minimally a host-based firewall] at [system components where host-based boundary protection mechanisms are to be implemented are defined;].

|  |
| --- |
| **SC-7(12) Control Summary Information** |
| Responsible Roles: Logging and Monitoring, Networking |
| Parameter sc-07.12\_odp.01: Packet Filtering, Firewalls, Event Reporting, Vulnerability Scanning Tools |
| Parameter sc-07.12\_odp.02: all servers in the Azure environment |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SC-7(12) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for implementing host-based boundary protection at customer-deployed virtual machines running customer-controlled operating systems.  **Azure**  Azure implements the following host-based boundary protection mechanisms:  \* IP Filtering  \* VFP Filtering (for virtual machines)  \* Host-based firewalls  \* Guest firewalls (for virtual machines)  Azure uses a combination of detection and fast response via several methods to address the risk of intrusion. This includes the use of event forwarding tools, security incident and event management tools, vulnerability scanning and reporting tools, and centrally managed antivirus and anti-malware on Azure assets. These tools are forms of host-based protection. |

### SC-7(18) - Fail Secure

Prevent systems from entering unsecure states in the event of an operational failure of a boundary protection device.

|  |
| --- |
| **SC-7(18) Control Summary Information** |
| Responsible Roles: Networking |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SC-7(18) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for preventing systems from entering unsecure states in the event of an operational failure of a boundary protection device.  **Azure**  Azure deploys geographically separate and redundant boundary protection network devices and Jumpboxesand SSL VPN servers. When an asset fails, it fails securely, and access is restricted to the environment. If Azure network devices, including but not limited to edge routers, access routers, load balancers, aggregation switches, and TORS fail, the affected circuit becomes disconnected, thereby failing securely. A failure of an Azure network device cannot lead to, or cause, information external to the system entering the device, nor can a failure permit unauthorized information release. The built-in redundancy allows Azure assets to fail without influencing availability. Many Azure network devices are configured to reboot in the event of failure, rather than remaining offline. |

### SC-7(20) - Dynamic Isolation and Segregation

Provide the capability to dynamically isolate [system components to be dynamically isolated from other system components are defined;] from other system components.

|  |
| --- |
| **SC-7(20) Control Summary Information** |
| Responsible Roles: Networking |
| Parameter sc-07.20\_odp: servers and network devices |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SC-7(20) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for ensuring that the system has the capability to dynamically isolate customer-deployed resources.  **Azure**  Azure personnel have the capability to isolate or segregate Azure assets by various means, including but not limited to:  \* Physical network disconnection  \* Removal from load balancer rotation  \* VLAN, NSG, and ACL isolation  Any of these actions can be performed in real time by the appropriate service team or Security Response Team as required. |

### SC-7(21) - Isolation of System Components

Employ boundary protection mechanisms to isolate [system components to be isolated by boundary protection mechanisms are defined;] supporting [missions and/or business functions to be supported by system components isolated by boundary protection mechanisms are defined;].

|  |
| --- |
| **SC-7(21) Control Summary Information** |
| Responsible Roles: Networking |
| Parameter sc-07.21\_odp.01: Service team systems |
| Parameter sc-07.21\_odp.02: Azure operations |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SC-7(21) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for employing boundary protection mechanisms to separate customer-defined resources supporting organizational missions and/or business functions.  **Azure**  Azure service teams are segregated from each other using Azure-managed boundary protection devices for bare metal hardware or logical isolation mechanisms for virtual machines, including VLAN and Network Security Group (NSG) and Virtual Network (VNet) segmentation, ACL restrictions, and encrypted communications. Azure also implements logical separation for its separate cloud environments in addition to all boundary protection mechanisms described above. |

## SC-8 Transmission Confidentiality and Integrity

Protect the [Selection (OneOrMore): confidentiality;integrity] of transmitted information.

Guidance: For each instance of data in transit, confidentiality AND integrity should be through cryptography as specified in SC-8 (1), physical means as specified in SC-8 (5), or in combination. For clarity, this control applies to all data in transit. Examples include the following data flows: \* Crossing the system boundary \* Between compute instances - including containers \* From a compute instance to storage \* Replication between availability zones \* Transmission of backups to storage \* From a load balancer to a compute instance \* Flows from management tools required for their work - e.g. log collection, scanning, etc. The following applies only when choosing SC-8 (5) in lieu of SC-8 (1). FedRAMP-Defined Assignment / Selection Parameters SC-8 (5)-1 [a hardened or alarmed carrier Protective Distribution System (PDS) when outside of Controlled Access Area (CAA)] SC-8 (5)-2 [prevent unauthorized disclosure of information AND detect changes to information]

Guidance: SC-8 (5) applies when physical protection has been selected as the method to protect confidentiality and integrity. For physical protection, data in transit must be in either a Controlled Access Area (CAA), or a Hardened or alarmed PDS. Hardened or alarmed PDS: Shall be as defined in SECTION X - CATEGORY 2 PDS INSTALLATION GUIDANCE of CNSSI No.7003, titled PROTECTED DISTRIBUTION SYSTEMS (PDS). Per the CNSSI No. 7003 Section VIII, PDS must originate and terminate in a Controlled Access Area (CAA). Controlled Access Area (CAA): Data will be considered physically protected, and in a CAA if it meets Section 2.3 of the DHS's Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies. CSPs can meet Section 2.3 of the DHS' recommended practice by satisfactory implementation of the following controls PE-2 (1), PE-2 (2), PE-2 (3), PE-3 (2), PE-3 (3), PE-6 (2), and PE-6 (3). Note: When selecting SC-8 (5), the above SC-8(5), and the above referenced PE controls must be added to the SSP. CNSSI No.7003 can be accessed here: https://www.dcsa.mil/Portals/91/documents/ctp/nao/CNSSI\_7003\_PDS\_September\_2015.pdf DHS Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies can be accessed here: https://us-cert.cisa.gov/sites/default/files/FactSheets/NCCIC%20ICS\_FactSheet\_Defense\_in\_Depth\_Strategies\_S508C.pdf

|  |
| --- |
| **SC-8 Control Summary Information** |
| Responsible Roles: Networking, SDL |
| Parameter sc-8: confidentiality and integrity |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SC-8 What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for configuring all customer-deployed resources to communicate through FIPS 140-2 validated encryption to protect the confidentiality and integrity of the information being transmitted.  Customers are responsible for configuring their web browsers, mobile devices, etc., to enable communications through FIPS 140-2 validated encryption. Customers who enforce FDCC/USGCB settings will achieve FIPS 140-2 encryption for data transmitted to Azure and between their enablers and the Azure web services interface; strong encryption with FIPS-approved ciphers is still possible if workstations are not operating in FIPS mode.  **Azure**  Azure services always use secure transport such as TLS or HTTPS. Encryption in transport is addressed by the transport protocol. Azure implements the transmission integrity and confidentiality control by ensuring that cryptography is implemented through a hybrid model. The following is a high-level list of the symmetric and asymmetric keys used for encrypting and protecting confidentiality of data.  \* AES for symmetric encryption/decryption  \* 128-bit or better symmetric keys  \* RSA for asymmetric encryption/decryption and signatures  \* 2048-bit or better RSA keys  \* SHA-256 or better (SHA-384, SHA-512) for hashing and message-authentication codes  Azure implements cryptography in numerous ways. Communications between the Azure service and the Azure Management Portal are configured to accept Federal Information Processing Standards (FIPS) 140-2 validated encryption. Azure enforces communications between Azure internal components to be protected with self-signed SSL certificates. Hardware Security Modules used by Azure Key Vault employ Federal Information Processing Standards (FIPS) 140-2 validated encryption. Azure requires that data is classified according to sensitivity (LBI, MBI, or HBI), and the owner of the data is responsible for following the Asset Classification Standard and Asset Protection Standard for encrypting data according to its classification.  Secrets are communicated through the Azure Management Portal and API over a secure TLS 1.2/1.3 channel. Both the SMAPI and the Azure Management Portal are only accessible over HTTPS. Service certificates, RDP passwords, and Storage Account Keys (SAKs) are stored in an encrypted format.  Azure utilizes Federal Information Processing Standards (FIPS) 140-2 Cryptographic Module Verification Program (CMVP) validated modules for areas requiring encryption. HMAC is keyed hash function for message authentication (RFC 2104). It makes use of an underlying hash function (MD5, SHA-1 or SHA-2) and a secret key of a specified length. The strength of an HMAC relies on the strength of the underlying hash function, and the length of the secret.  \* A SHA-2 hash is required for new code.  \* SHA-1 is permissible in existing code only for backwards compatibility and after review by the Crypto Board.  \* MAC3DES is permissible for managed code only since this is the only FIPS-compliant keyed hash algorithm for .NET currently available. A Crypto Board review is required for such usage.  \* Other hash functions, including MD2, MD4 or MD5 are not permitted, and must be replaced in existing code.  All approved keyed hash algorithms are members of the HMAC family. HMAC is a mechanism for constructing a keyed hash algorithm using an underlying hash algorithm. For projects utilizing keyed hash algorithms, the following hash functions must be used within the HMAC mechanism.  Note that hash function agility (the ability to switch to another hash function without patching the code) is part of the “Implement Crypto Agility” requirement. No new code should use the MD4 or MD5 hash algorithms as hash collisions have been demonstrated for both algorithms. SHA1 is being deprecated. Continued use of SHA-1 is permissible in existing code only for backwards compatibility and, as described below, for new code running on certain down-level platforms. A SHA-2 hash is currently the only recommended hash function. The SHA-2 hash functions are available in managed code, and in unmanaged code targeting Windows Server 2003 SP1 and later versions of Windows.  For new managed code, use of a SHA-2 hash function is required. SHA-1 is permissible in existing code only for backwards compatibility. Such usage requires Crypto Board review. All other hash functions, including MD2, MD4 or MD5 must not be used, and must be replaced in existing code. For unmanaged code, use of a SHA-2 hash function is required.  In order to access the Azure environment via network connection, a user must authenticate with their Azure domain credentials. Azure provides access through smart-card-enabled Jumpboxesand SSL VPN servers when establishing access connections into the Azure environments. Users must have a valid smart card, and valid Azure domain accounts to establish a remote access session. Jumpboxesand SSL VPN servers are configured to use the Federal Information Processing Standards (FIPS) 140-2 encryption setting, specifically TLS 1.2/1.3.  The use of Federal Information Processing Standards (FIPS) 140-2 validated cryptography is used by Azure to support compliance with federal laws, executive orders, directives, policies, regulations, standards, and guidance. Federal Information Processing Standards (FIPS) 140-2 encryption is required for digital media physically transported, electronically transmitted over Azure via TLS, and for authentication for Windows-based authentication and SSH authentication to network devices.  Encrypted data may transit across the Azure environment, but the network devices are agnostic as to the type of data being transmitted. Azure relies on extensive physical security to protect all the end to end communications inside datacenters.  Note that Azure does not have email or fax machines in the Azure boundary, and thus the MARS-E MP-CMS-1, SC-ACA-1, and SC-ACA-2 requirements are a customer responsibility. |

### SC-8(1) - Cryptographic Protection

Implement cryptographic mechanisms to [Selection (OneOrMore): prevent unauthorized disclosure of information;detect changes to information] during transmission.

Requirement: Please ensure SSP Section 10.3 Cryptographic Modules Implemented for Data At Rest (DAR) and Data In Transit (DIT) is fully populated for reference in this control.

Guidance: See M-22-09, including \"Agencies encrypt all DNS requests and HTTP traffic within their environment\" SC-8 (1) applies when encryption has been selected as the method to protect confidentiality and integrity. Otherwise refer to SC-8 (5). SC-8 (1) is strongly encouraged.

Guidance: Note that this enhancement requires the use of cryptography which must be compliant with Federal requirements and utilize FIPS validated or NSA approved cryptography (see SC-13.)

Guidance: When leveraging encryption from the underlying IaaS/PaaS: While some IaaS/PaaS services provide encryption by default, many require encryption to be configured, and enabled by the customer. The CSP has the responsibility to verify encryption is properly configured.

|  |
| --- |
| **SC-8(1) Control Summary Information** |
| Responsible Roles: Networking, SDL |
| Parameter sc-08.01\_odp: prevent unauthorized disclosure of information AND detect changes to information |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SC-8(1) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for implementing cryptographic mechanisms to prevent unauthorized disclosure of information and/or detect changes to information during transmission.  **Azure**  Azure uses encryption to prevent unauthorized disclosure of information and detect changes to information during transmission. Specifically, Azure provides Federal Information Processing Standards (FIPS) 140-2 compliant ciphers that include integrity validation for customer connections, interconnected system connections, and remote access connections.  For connections to customers, Azure is configured to negotiate FIPS compliant TLS protocols with supported client browsers, though non-FIPS compliant protocols are supported for legacy browser support.  Connections within the accreditation boundary occur within Azure facilities. Since Azure owns and controls access to these connections, they do not require Federal Information Processing Standards (FIPS) 140-2 encryption. However, service-to-service communications occur over TLS 1.2/1.3, and internal communication between Azure datacenters is transmitted over Federal Information Processing Standards (FIPS) 140-2 compliant AES 256 link encryptors to the ensure confidentiality of data. |

## SC-10 Network Disconnect

Terminate the network connection associated with a communications session at the end of the session or after [no longer than ten (10) minutes for privileged sessions and no longer than fifteen (15) minutes for user sessions] of inactivity.

|  |
| --- |
| **SC-10 Control Summary Information** |
| Responsible Roles: JIT, Networking, VPN, Jumpbox |
| Parameter sc-10: SAW workstations is at 10 minutes, SAW VPN is at 360 minutes, non-SAW VPN is at 60 minutes, RDP for servers is at 1 hour and 1 day, SSH for servers is at 15 minutes, and SSH for network devices is at 60 minute |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☒ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SC-10 What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for implementing a network disconnect for customer-deployed resources at the end of a communication session or after a customer-defined time period of inactivity.  **Azure**  Azure Secure Admin Workstations (SAWs) require re-authentication after at most ten (10) minutes of user inactivity. These are the only method of access to the environment. The SAW VPN terminates inactive sessions after three hundred sixty (360) minutes of inactivity, and the non-SAW VPN terminates inactive sessions after sixty (60) minutes of inactivity.  The logical access process to Azure resources is controlled using Remote Desktop Protocol (RDP), Secure Shell (SSH) and the SSL VPN. Non-interactive sessions are not permitted through Azure.  **Servers**  RDP and SSH idle timeout inherit the settings of the target server. Azure servers are configured to terminate idle sessions after one (1) hour of inactivity and one (1) day to end a disconnected session for RDP and (15) minutes of inactivity for SSH.  **Network Devices**  SSH idle timeout inherits the settings of the target network device. Azure network devices are configured to terminate inactive sessions after sixty (60) minutes.  Azure implements user sessions that terminate after sixty (60) minutes of inactivity on the VPN. The risks associated with a sixty (60) minute disconnect are mitigated through using multifactor authentication (MFA) with Federal Information Processing Standards (FIPS) 140-2 level 3 validated smart card tokens for all in-band management and by logging security events related to account activity. |

## SC-12 Cryptographic Key Establishment and Management

Establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: [In accordance with Federal requirements].

Guidance: See references in NIST 800-53 documentation.

Guidance: Must meet applicable Federal Cryptographic Requirements. See References Section of control.

Guidance: Wildcard certificates may be used internally within the system, but are not permitted for external customer access to the system.

|  |
| --- |
| **SC-12 Control Summary Information** |
| Responsible Roles: Secret Management Stores |
| Parameter sc-12: the Public Key Infrastructure Operational Security Standard |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SC-12 What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for managing cryptographic keys used within customer-deployed resources in accordance with customer-defined requirements for key generation, distribution, storage, access, and destruction.  Government user entities will ensure that personal computing devices (client systems) are configured to request FIPS 140-2 encryption ciphers and protocols for all network sessions.sessions.  **Azure**  When cryptographic capabilities are employed to protect the confidentiality, integrity, or availability of data within Azure, the algorithms and cryptographic modules are Federal Information Processing Standards (FIPS) 140-2 compliant. Rather than validate individual services, components, or products, Microsoft chooses to validate only the underlying cryptographic modules. Subsequently, Azure services are built to rely on the Federal Information Processing Standards (FIPS) 140-2 validated cryptographic modules of the underlying operating systems, including the Cryptographic API: Next Generation (CNG) and Cryptographic API (CAPI) for Windows and Kernel Crypto API for Linux. Azure uses the documented APIs for each of the modules to access various cryptographic services. For additional information on how cryptographic modules are employed in Microsoft products, see the links below:  <https://docs.microsoft.com/en-us/windows/security/threat-protection/fips-140-validation>  <https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-fips-140-2>  When utilizing cryptographic mechanisms for securing data or services, Azure adheres to Microsoft’s Key Management Standard for establishing and managing keys. The Key Management Standard applies to all environments managed by Azure, including labs, production, and preproduction. Equipment used to generate, store and archive keys is physically and logically protected. Keys are classified and destroyed in accordance with the requirements set forth in the Asset Classification Standard and Asset Protection Standard documents. To reduce the likelihood of compromise, activation and deactivation dates for keys are defined so that the keys can only be used for a limited period. The Key Management Standard mandates the following Key Management Procedures:  \* Standard Operating Procedures  \* Secure methods  \* Storing Keys  \* Distributing Keys  \* Archiving Keys  \* Key Destruction  \* Changing or Updating Keys  \* Compromised Keys  \* Recovering Keys  \* Revoking Keys  \* Logging and Auditing  \* Key Distribution and access control  Azure implements cryptographic key management through the use of approved secret stores, including Azure Key Vault and dSMS. Azure ensures that both secret stores contain the approved trust anchors, including certificates with visibility external to Azure and certificates related to the internal operations of services.  **Servers**  Azure leverages the cryptographic capabilities that are directly a part of the Windows and Linux operating systems for certificates and authentication mechanisms such as Kerberos v5. These cryptographic modules have been certified by NIST as being Federal Information Processing Standards (FIPS) 140-2 compliant.  \* 3651 - Secure Kernel Code Integrity  \* 3644 - Code Integrity  \* 3615 - Windows OS Loader  \* 3527 - Kernel Mode Cryptographic Primitives Library  \* 3513 - Secure Kernel Code Integrity (skci.dll) in Windows 10 Pro, Windows 10 Enterprise, Windows 10 Enterprise LTSB, Windows Server 2016 Standard, Windows Server 2016 Datacenter, Windows Storage Server 2016  \* 3510 - Code Integrity (ci.dll) in Microsoft Windows 10, Windows 10 Pro, Windows 10 Enterprise, Windows 10 Enterprise LTSB, Windows 10 Mobile, Windows Server 2016 Standard, Windows Server 2016 Datacenter, Windows Storage Server 2016  \* 3502 - BitLocker® Windows OS Loader (winload) in Microsoft Windows 10, Windows 10 Pro, Windows 10 Enterprise, Windows 10 Enterprise LTSB, Windows 10 Mobile, Windows Server 2016 Standard, Windows Server 2016 Datacenter, Windows Storage Server 2016  \* 3501 - BitLocker® Windows Resume (winresume) in Microsoft Windows 10, Windows 10 Pro, Windows 10 Enterprise, Windows 10 Enterprise LTSB, Windows Server 2016 Standard, Windows Server 2016 Datacenter, Windows Storage Server 2016  \* 3487 - Boot Manager in Microsoft Windows 10, Windows 10 Pro, Windows 10 Enterprise, Windows 10 Enterprise LTSB, Windows 10 Mobile, Windows Server 2016 Standard, Windows Server 2016 Datacenter, Windows Storage Server 2016  \* 3480 - Windows OS Loader  \* 3690 - Virtual TPM  \* 3197 - Cryptographic Primitives Library  \* 3196 - Kernel Mode Cryptographic Primitives Library  \* 3195 - Code Integrity  \* 3194 - Windows OS Loader  \* 3096 - Secure Kernel Code Integrity  \* 3095 - Cryptographic Primitives Library  \* 3094 - Kernel Mode Cryptographic Primitives Library  \* 3093 - Code Integrity  \* 3092 - BitLocker Dump Filter  \* 3091 - Windows Resume  \* 3090 - Windows OS Loader  \* 3089 - Boot Manager  \* 2938 - Secure Kernel Code Integrity (skci.dll) in Windows 10 Pro, Windows 10 Enterprise, Windows 10 Enterprise LTSB, Windows Server 2016 Standard, Windows Server 2016 Datacenter, Windows Storage Server 2016  \* 2937 - Cryptographic Primitives Library (bcryptprimitives.dll and ncryptsslp.dll) in Microsoft Windows 10, Windows 10 Pro, Windows 10 Enterprise, Windows 10 Enterprise LTSB, Windows 10 Mobile, Windows Server 2016 Standard, Windows Server 2016 Datacenter, Windows Storage Server 2016, Azure Host OS (version 1.65)  \* 2936 - Kernel Mode Cryptographic Primitives Library (cng.sys) in Microsoft Windows 10, Windows 10 Pro, Windows 10 Enterprise, Windows 10 Enterprise LTSB, Windows 10 Mobile, Windows Server 2016 Standard, Windows Server 2016 Datacenter, Windows Storage Server 2016, Azure Host OS (version 1.65)  \* 2935 - Code Integrity (ci.dll) in Microsoft Windows 10, Windows 10 Pro, Windows 10 Enterprise, Windows 10 Enterprise LTSB, Windows 10 Mobile, Windows Server 2016 Standard, Windows Server 2016 Datacenter, Windows Storage Server 2016, Azure Host OS (version 1.65)  \* 2934 - BitLocker® Dump Filter (dumpfve.sys) in Windows 10 Pro, Windows 10 Enterprise, Windows 10 Enterprise LTSB, Windows 10 Mobile, Windows Server 2016 Standard, Windows Server 2016 Datacenter, Windows Storage Server 2016, Azure Host OS (version 1.65)  \* 2933 - BitLocker® Windows Resume (winresume) in Microsoft Windows 10, Windows 10 Pro, Windows 10 Enterprise, Windows 10 Enterprise LTSB, Windows Server 2016 Standard, Windows Server 2016 Datacenter, Windows Storage Server 2016  \* 2932 - BitLocker® Windows OS Loader (winload) in Microsoft Windows 10, Windows 10 Pro, Windows 10 Enterprise, Windows 10 Enterprise LTSB, Windows 10 Mobile, Windows Server 2016 Standard, Windows Server 2016 Datacenter, Windows Storage Server 2016, Azure Host OS (version 1.65)  \* 2931 - Boot Manager in Microsoft Windows 10, Windows 10 Pro, Windows 10 Enterprise, Windows 10 Enterprise LTSB, Windows 10 Mobile, Windows Server 2016 Standard, Windows Server 2016 Datacenter, Windows Storage Server 2016, Azure Host OS (version 1.65)  \* 2357 - Cryptographic Primitives Library (bcryptprimitives.dll and ncryptsslp.dll) in Microsoft Windows 8.1 Enterprise, Windows Server 2012 R2, Windows Storage Server 2012 R2, Surface Pro 3, Surface Pro 2, Surface Pro, Surface 2, Surface, Windows RT 8.1, Windows Phone 8.1, Windows Embedded 8.1 Industry Enterprise, StorSimple 8000 Series, Azure StorSimple Virtual Array Windows Server 2012 R2  \* 2356 - Kernel Mode Cryptographic Primitives Library (cng.sys) in Microsoft Windows 8.1 Enterprise, Windows Server 2012 R2, Windows Storage Server 2012 R2, Surface Pro 3, Surface Pro 2, Surface Pro, Surface 2, Surface, Windows RT 8.1, Windows Phone 8.1, Windows Embedded 8.1 Industry Enterprise, StorSimple 8000 Series, Azure StorSimple Virtual Array Windows Server 2012 R2  \* 2355 - Code Integrity (ci.dll) in Microsoft Windows 8.1 Enterprise, Windows Server 2012 R2, Windows Storage Server 2012 R2, Surface Pro 3, Surface Pro 2, Surface Pro, Surface 2, Surface, Windows RT 8.1, Windows Phone 8.1, Windows Embedded 8.1 Industry Enterprise, StorSimple 8000 Series, Azure StorSimple Virtual Array Windows Server 2012 R2  \* 2354 - BitLocker® Dump Filter (dumpfve.sys) in Microsoft Windows 8.1 Enterprise, Windows Server 2012 R2, Windows Storage Server 2012 R2, Surface Pro 3, Surface Pro 2, Surface Pro,Surface 2, Surface, Windows RT 8.1, Windows Phone 8.1, Windows Embedded 8.1 Industry Enterprise, StorSimple 8000 Series  \* 2353 - BitLocker® Windows Resume (winresume) in Microsoft Windows 8.1 Enterprise, Windows Server 2012 R2, Windows Storage Server 2012 R2, Surface Pro 3, Surface Pro 2, Surface Pro, Windows Embedded 8.1 Industry Enterprise, StorSimple 8000 Series  \* 2352 - BitLocker® Windows OS Loader (winload) in Microsoft Windows 8.1 Enterprise, Windows Server 2012 R2, Windows Storage Server 2012 R2, Surface Pro 3, Surface Pro 2, Surface Pro, Surface 2, Surface, Windows RT 8.1, Windows Phone 8.1, Windows Embedded 8.1 Industry Enterprise, StorSimple 8000 Series, Azure StorSimple Virtual Array Windows Server 2012 R2  \* 2351 - Boot Manager in Microsoft Windows 8.1 Enterprise, Windows Server 2012 R2, Windows Storage Server 2012 R2, Surface Pro 3, Surface Pro 2, Surface Pro, Surface 2, Surface, Windows RT 8.1, Windows Phone 8.1, Windows Embedded 8.1 Industry Enterprise, StorSimple 8000 Series, Azure StorSimple Virtual Array Windows Server 2012 R2  \* 3651 - Secure Kernel Code Integrity  \* 3644 - Code Integrity  \* 3615 - Windows OS Loader  \* 3197 - Cryptographic Primitives Library  \* 3196 - Kernel Mode Cryptographic Primitives Library  \* 3092 - BitLocker Dump Filter  \* 3089 - Boot Manager  The Linux servers employ NIST-certified Federal Information Processing Standards (FIPS) 140-2 compliant cryptographic modules.  \* 3647 - Ubuntu 18.04 Kernel Crypto API Cryptographic Module  \* 3622 - Ubuntu 18.04 OpenSSL Cryptographic Module  \* 3633 - Ubuntu 18.04 OpenSSH Client Cryptographic Module  \* 3632 - Ubuntu 18.04 OpenSSH Server Cryptographic Module  \* 3648 - Ubuntu 18.04 Strongswan Cryptographic Module  \* 3683 - Ubuntu 18.04 Azure Kernel Crypto API Cryptographic Module  \* 2962 - Ubuntu Kernel Crypto API Cryptographic Module  \* 2888 - Ubuntu OpenSSL Cryptographic Module  \* 2907 - Ubuntu OpenSSH Client Cryptographic Module  \* 2906 - Ubuntu OpenSSH Server Cryptographic Module  \* 2978 - Ubuntu Strongswan Cryptographic Module  \* 4277 - Microsoft Azure Linux Kernel Crypto API (Formerly CBL-Mariner 1.0 Kernel Crypto API)  \* 4496 - Microsoft Azure Linux OpenSSL Cryptographic Library (Formerly CBL-Mariner 2.0 OpenSSL Cryptographic Module)  \* 4292 - Ubuntu 20.04 OpenSSL Cryptographic Module  \* 4126 - Ubuntu 20.04 Azure Kernel Crypto API Cryptographic Module  \* 4046 - Ubuntu 20.04 Strongswan Cryptographic Module  \* 3966 - Ubuntu 20.04 OpenSSL Cryptographic Module  \* 3928 - Ubuntu 20.04 Kernel Crypto API Cryptographic Module"  \* 3902 - Ubuntu 20.04 Libgcrypt Cryptographic Module  \* 3939 - Red Hat Enterprise Linux 7 Kernel Crypto API Cryptographic Module"  \* 3725 - Ubuntu 16.04 OpenSSL Cryptographic Module"  \* 3724 - Ubuntu 16.04 Kernel Crypto API Cryptographic Module  \* 3980 - Ubuntu 18.04 OpenSSL Cryptographic Module  \* 3876 - Red Hat Enterprise Linux 7 OpenSSL Cryptographic Module"  \* 3538 - Red Hat Enterprise Linux OpenSSL Cryptographic Module"  \* 3016 - Red Hat Enterprise Linux OpenSSL Cryptographic Module"  \* 4642 - Red Hat Enterprise Linux 8 OpenSSL Cryptographic Module  \* 4458 - Red Hat Enterprise Linux 8 NSS Cryptographic Module  \* 4438 - Red Hat Enterprise Linux 8 libgcrypt Cryptographic Module  \* 4434 - Red Hat Enterprise Linux 8 Kernel Crypto API Cryptographic Module  \* 4428 - Red Hat Enterprise Linux 8 GnuTLS Cryptographic Module  \* 4413 - Red Hat Enterprise Linux 8 NSS Cryptographic Module  \* 4397- Red Hat Enterprise Linux 8 libgcrypt Cryptographic Module  \* 4384 - Red Hat Enterprise Linux 8 libgcrypt Cryptographic Module  \* 4272 - Red Hat Enterprise Linux 8 GnuTLS Cryptographic Module  \* 4271 - Red Hat Enterprise Linux 8 OpenSSL Cryptographic Module  \* 4254 - Red Hat Enterprise Linux 8 Kernel Crypto API Cryptographic Module  \* 3784 - Red Hat Enterprise Linux 8 libgcrypt Cryptographic Module  \* 3956 - Red Hat Enterprise Linux 8 GnuTLS Cryptographic Module  \* 3946 - Red Hat Enterprise Linux 8 NSS Cryptographic Module  \* 3918 - Red Hat Enterprise Linux 8 Kernel Crypto API Cryptographic Module  \* 3842 - Red Hat Enterprise Linux 8 OpenSSL Cryptographic Module  \* 3839 - Red Hat Enterprise Linux 8 NSS Cryptographic Module  \* 3813 - Red Hat Enterprise Linux 8 GnuTLS Cryptographic Module  \* 3794 - Red Hat Enterprise Linux 8 Kernel Crypto API Cryptographic Module  \* 3781 - Red Hat Enterprise Linux 8 OpenSSL Cryptographic Module  \* 3892 - Red Hat Enterprise Linux 7 OpenSSH Client Cryptographic Module  \* 3891 - Red Hat Enterprise Linux 7 OpenSSH Server Cryptographic Module  \* 3867 - Red Hat Enterprise Linux 7 OpenSSL Cryptographic Module  \* 3860 - Red Hat Enterprise Linux 7 NSS Cryptographic Module  \* 3563 - Red Hat Enterprise Linux 7 Libreswan Cryptographic Module  \* 2441 - Red Hat Enterprise Linux 6.6 OpenSSL Module, Red Hat Enterprise Linux 7.1 OpenSSL Module  \* 4498 - Red Hat Enterprise Linux 7 NSS Cryptographic Module  \* 4282 - OpenSSL FIPS Provider  **Network Devices**  Encrypted data may transit across the Azure network, but the network devices are agnostic as to the type of data being transmitted. Network devices use the following cryptographic modules:  \* 2984 - Cisco FIPS Object Module  \* 2505 - Cisco FIPS Object Module  \* 3429 - EOS MACsec Alpha Hybrid Module  \* 3420 - EOS MACsec Bravo Hybrid Module  \* 2909 - Arista EOS Crypto Module v1.0  \* 3621 - Juniper Networks MX80, MX104, MX240, MX480, MX960 3D Universal Edge Routers with RE-S-X6-64G/RE-S-X6-128G Routing Engine and MIC-MACsec-20GE MACSec Card  \* 2921 - Juniper Networks SRX1400, SRX3400, and SRX3600 Services Gateways  \* 3629 - F5® Device Cryptographic Module  \* 2988 - Citrix FIPS Cryptographic Module  \* 4019 - Arista EOS Crypto Module  \* 1521 - Cisco 2951, Cisco 3925 and Cisco 3945 Integrated Services Routers (ISRs)  \* 2409 - Cisco ASR 1001, 1001-X, 1002, 1002-X, 1004, 1006 and 1013  \* 2090 - Cisco ASR 1001, ASR 1002, ASR1002-X, ASR 1006, and ASR 1013  \* 3775 - Cisco ASR 1000 Series Routers with MACsec  \* 3988 - Cisco ASR 1000 Series Routers without MACsec  \* 3841 - F5® Device Cryptographic Module"  \* 2896 - Pulse Secure Cryptographic Module  \* 3416 - Juniper Networks MX240, MX480, MX960, MX2010, MX2020 3D Universal Edge Routers and EX9204, EX9208, EX9214 Ethernet Switches with RE1800 Routing Engine  \* 3934 - Juniper Networks MX240, MX480, MX960 3D Universal Edge Routers with RE1800 Routing Engine and Multiservices MPC  \* 3935 - Juniper Networks MX240, MX480, MX960 3D Universal Edge Routers with RE1800 Routing Engine and MPC7E-10G MACsec Card  \* 2388 - IOS Common Cryptographic Module (IC2M) Rel5  AES-256 bit encrypted SSH is used for network device authentication using Federal Information Processing Standards (FIPS) 140-2 approved algorithms:  \* 0048 - SecureCRT VanDyke 8.0.3 (FIPS Validation Certificate 0048)  \* 2643 - nShield F2 500+, nShield F2 1500+ and nShield F2 6000+  **Azure Key Stores**  The Thales nShield Hardware Security Modules used by KeyVault employ cryptographic modules certified by NIST as being Federal Information Processing Standards (FIPS) 140-2 compliant; relevant NIST certificate number is 2643. Azure Managed HSM and KeyVault utilize CMVP certificate number 4399 from Marvell vendor. Azure Dedicated HSM utilizes CMVP certificate numbers 4090 and 4684 certificate numbers from Thales vendor. Azure leverages the NIST CMVP certificate numbers 3517, 3914, and 3907 for Yubico, Inc. cryptographic modules to enable multi-factor authentication within Azure cloud production environments. |

### SC-12(1) - Availability

Maintain availability of information in the event of the loss of cryptographic keys by users.

|  |
| --- |
| **SC-12(1) Control Summary Information** |
| Responsible Roles: Secret Management Stores, Storage |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SC-12(1) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for maintaining the availability of information in the event of the loss of cryptographic keys by users.  **Azure**  Azure stores all Storage Account Keys within an approved secret management store, which tracks and monitors access to secrets. The approved secret management stores, Key Vault and dSMS, are backed up regularly and provide the ability to restore data that has been accidentally deleted. This ensures that the Storage Account Key is never lost. Azure Storage also has a soft delete option, which preserves a key if accidentally or maliciously deleted. |

## SC-13 Cryptographic Protection

a. Determine the [cryptographic uses are defined;] ; and

b. Implement the following types of cryptography required for each specified cryptographic use: [FIPS-validated or NSA-approved cryptography].

Guidance: This control applies to all use of cryptography. In addition to encryption, this includes functions such as hashing, random number generation, and key generation. Examples include the following: \* Encryption of data \* Decryption of data \* Generation of one time passwords (OTPs) for MFA \* Protocols such as TLS, SSH, and HTTPS The requirement for FIPS 140 validation, as well as timelines for acceptance of FIPS 140-2, and 140-3 can be found at the NIST Cryptographic Module Validation Program (CMVP). https://csrc.nist.gov/projects/cryptographic-module-validation-program

Guidance: For NSA-approved cryptography, the National Information Assurance Partnership (NIAP) oversees a national program to evaluate Commercial IT Products for Use in National Security Systems. The NIAP Product Compliant List can be found at the following location: https://www.niap-ccevs.org/Product/index.cfm

Guidance: When leveraging encryption from underlying IaaS/PaaS: While some IaaS/PaaS provide encryption by default, many require encryption to be configured, and enabled by the customer. The CSP has the responsibility to verify encryption is properly configured.

Guidance: Moving to non-FIPS CM or product is acceptable when: \* FIPS validated version has a known vulnerability \* Feature with vulnerability is in use \* Non-FIPS version fixes the vulnerability \* Non-FIPS version is submitted to NIST for FIPS validation \* POA&M is added to track approval, and deployment when ready

Guidance: At a minimum, this control applies to cryptography in use for the following controls: AU-9(3), CP-9(8), IA-2(6), IA-5(1), MP-5, SC-8(1), and SC-28(1).

|  |
| --- |
| **SC-13 Control Summary Information** |
| Responsible Roles: Secret Management Stores, SDL |
| Parameter sc-13\_odp.01: organization-defined cryptographic uses |
| Parameter sc-13\_odp.02: FIPS-validated or NSA-approved cryptography |
| Implementation Status (check all that apply):  ☐ Implemented  ☒ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SC-13 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for determining organization-defined cryptographic uses.  **Azure**  Azure uses cryptography for the protection of controlled unclassified information, provision and implementation of digital signatures, logical network separation, and random number and hash generation. |
| **Part B**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for implementing customer-defined cryptography within customer-deployed resources in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.  Government customers will ensure that personal computing devices (client systems) are configured to request FIPS 140-2 encryption ciphers and protocols for all network sessions. Commercial customers may also choose to use FIPS 140-2 ciphers and protocols when connecting to Azure Public.  **Azure**  Encryption mechanisms and techniques used within Azure follow the requirements and restrictions outlined in the Microsoft Key Management Standard, Microsoft Operational Encryption Standard, Azure Cryptographic Controls Standard Operating Procedure. The Microsoft Key Management Standard applies to the operation of all Microsoft’s online services residing within Azure utilizing cryptographic mechanisms for securing data or services. This standard applies to all environments managed by Azure, including labs, production, and pre-production.  Azure implements cryptography through encryption mechanisms and techniques following the requirements outlined in the Cryptographic Controls of the Microsoft Security Program Policy (MSPP).  Federal Information Processing Standards (FIPS) 140-2 validated cryptographic modules are used to support compliance with federal laws, executive orders, directives, policies, regulations, and standards. Additional information can be found at the link below:  <https://docs.microsoft.com/en-us/windows/security/threat-protection/fips-140-validation>  Specific encryption modules being used and the certificates for the server baselines can be found at <https://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm> and are identified below, using the Certificate Number and Module Name.  **Servers**  Azure leverages the cryptographic capabilities that are directly a part of the Windows and Linux operating systems for certificates and authentication mechanisms such as Kerberos v5. These cryptographic modules have been certified by NIST as being Federal Information Processing Standards (FIPS) 140-2 compliant.  \* 3651 - Secure Kernel Code Integrity  \* 3644 - Code Integrity  \* 3615 - Windows OS Loader  \* 3527 - Kernel Mode Cryptographic Primitives Library  \* 3513 - Secure Kernel Code Integrity (skci.dll) in Windows 10 Pro, Windows 10 Enterprise, Windows 10 Enterprise LTSB, Windows Server 2016 Standard, Windows Server 2016 Datacenter, Windows Storage Server 2016  \* 3510 - Code Integrity (ci.dll) in Microsoft Windows 10, Windows 10 Pro, Windows 10 Enterprise, Windows 10 Enterprise LTSB, Windows 10 Mobile, Windows Server 2016 Standard, Windows Server 2016 Datacenter, Windows Storage Server 2016  \* 3502 - BitLocker® Windows OS Loader (winload) in Microsoft Windows 10, Windows 10 Pro, Windows 10 Enterprise, Windows 10 Enterprise LTSB, Windows 10 Mobile, Windows Server 2016 Standard, Windows Server 2016 Datacenter, Windows Storage Server 2016  \* 3501 - BitLocker® Windows Resume (winresume) in Microsoft Windows 10, Windows 10 Pro, Windows 10 Enterprise, Windows 10 Enterprise LTSB, Windows Server 2016 Standard, Windows Server 2016 Datacenter, Windows Storage Server 2016  \* 3487 - Boot Manager in Microsoft Windows 10, Windows 10 Pro, Windows 10 Enterprise, Windows 10 Enterprise LTSB, Windows 10 Mobile, Windows Server 2016 Standard, Windows Server 2016 Datacenter, Windows Storage Server 2016  \* 3480 - Windows OS Loader  \* 3690 - Virtual TPM  \* 3197 - Cryptographic Primitives Library  \* 3196 - Kernel Mode Cryptographic Primitives Library  \* 3195 - Code Integrity  \* 3194 - Windows OS Loader  \* 3096 - Secure Kernel Code Integrity  \* 3095 - Cryptographic Primitives Library  \* 3094 - Kernel Mode Cryptographic Primitives Library  \* 3093 - Code Integrity  \* 3092 - BitLocker Dump Filter  \* 3091 - Windows Resume  \* 3090 - Windows OS Loader  \* 3089 - Boot Manager  \* 2938 - Secure Kernel Code Integrity (skci.dll) in Windows 10 Pro, Windows 10 Enterprise, Windows 10 Enterprise LTSB, Windows Server 2016 Standard, Windows Server 2016 Datacenter, Windows Storage Server 2016  \* 2937 - Cryptographic Primitives Library (bcryptprimitives.dll and ncryptsslp.dll) in Microsoft Windows 10, Windows 10 Pro, Windows 10 Enterprise, Windows 10 Enterprise LTSB, Windows 10 Mobile, Windows Server 2016 Standard, Windows Server 2016 Datacenter, Windows Storage Server 2016, Azure Host OS (version 1.65)  \* 2936 - Kernel Mode Cryptographic Primitives Library (cng.sys) in Microsoft Windows 10, Windows 10 Pro, Windows 10 Enterprise, Windows 10 Enterprise LTSB, Windows 10 Mobile, Windows Server 2016 Standard, Windows Server 2016 Datacenter, Windows Storage Server 2016, Azure Host OS (version 1.65)  \* 2935 - Code Integrity (ci.dll) in Microsoft Windows 10, Windows 10 Pro, Windows 10 Enterprise, Windows 10 Enterprise LTSB, Windows 10 Mobile, Windows Server 2016 Standard, Windows Server 2016 Datacenter, Windows Storage Server 2016, Azure Host OS (version 1.65)  \* 2934 - BitLocker® Dump Filter (dumpfve.sys) in Windows 10 Pro, Windows 10 Enterprise, Windows 10 Enterprise LTSB, Windows 10 Mobile, Windows Server 2016 Standard, Windows Server 2016 Datacenter, Windows Storage Server 2016, Azure Host OS (version 1.65)  \* 2933 - BitLocker® Windows Resume (winresume) in Microsoft Windows 10, Windows 10 Pro, Windows 10 Enterprise, Windows 10 Enterprise LTSB, Windows Server 2016 Standard, Windows Server 2016 Datacenter, Windows Storage Server 2016  \* 2932 - BitLocker® Windows OS Loader (winload) in Microsoft Windows 10, Windows 10 Pro, Windows 10 Enterprise, Windows 10 Enterprise LTSB, Windows 10 Mobile, Windows Server 2016 Standard, Windows Server 2016 Datacenter, Windows Storage Server 2016, Azure Host OS (version 1.65)  \* 2931 - Boot Manager in Microsoft Windows 10, Windows 10 Pro, Windows 10 Enterprise, Windows 10 Enterprise LTSB, Windows 10 Mobile, Windows Server 2016 Standard, Windows Server 2016 Datacenter, Windows Storage Server 2016, Azure Host OS (version 1.65)  \* 2357 - Cryptographic Primitives Library (bcryptprimitives.dll and ncryptsslp.dll) in Microsoft Windows 8.1 Enterprise, Windows Server 2012 R2, Windows Storage Server 2012 R2, Surface Pro 3, Surface Pro 2, Surface Pro, Surface 2, Surface, Windows RT 8.1, Windows Phone 8.1, Windows Embedded 8.1 Industry Enterprise, StorSimple 8000 Series, Azure StorSimple Virtual Array Windows Server 2012 R2  \* 2356 - Kernel Mode Cryptographic Primitives Library (cng.sys) in Microsoft Windows 8.1 Enterprise, Windows Server 2012 R2, Windows Storage Server 2012 R2, Surface Pro 3, Surface Pro 2, Surface Pro, Surface 2, Surface, Windows RT 8.1, Windows Phone 8.1, Windows Embedded 8.1 Industry Enterprise, StorSimple 8000 Series, Azure StorSimple Virtual Array Windows Server 2012 R2  \* 2355 - Code Integrity (ci.dll) in Microsoft Windows 8.1 Enterprise, Windows Server 2012 R2, Windows Storage Server 2012 R2, Surface Pro 3, Surface Pro 2, Surface Pro, Surface 2, Surface, Windows RT 8.1, Windows Phone 8.1, Windows Embedded 8.1 Industry Enterprise, StorSimple 8000 Series, Azure StorSimple Virtual Array Windows Server 2012 R2  \* 2354 - BitLocker® Dump Filter (dumpfve.sys) in Microsoft Windows 8.1 Enterprise, Windows Server 2012 R2, Windows Storage Server 2012 R2, Surface Pro 3, Surface Pro 2, Surface Pro,Surface 2, Surface, Windows RT 8.1, Windows Phone 8.1, Windows Embedded 8.1 Industry Enterprise, StorSimple 8000 Series  \* 2353 - BitLocker® Windows Resume (winresume) in Microsoft Windows 8.1 Enterprise, Windows Server 2012 R2, Windows Storage Server 2012 R2, Surface Pro 3, Surface Pro 2, Surface Pro, Windows Embedded 8.1 Industry Enterprise, StorSimple 8000 Series  \* 2352 - BitLocker® Windows OS Loader (winload) in Microsoft Windows 8.1 Enterprise, Windows Server 2012 R2, Windows Storage Server 2012 R2, Surface Pro 3, Surface Pro 2, Surface Pro, Surface 2, Surface, Windows RT 8.1, Windows Phone 8.1, Windows Embedded 8.1 Industry Enterprise, StorSimple 8000 Series, Azure StorSimple Virtual Array Windows Server 2012 R2  \* 2351 - Boot Manager in Microsoft Windows 8.1 Enterprise, Windows Server 2012 R2, Windows Storage Server 2012 R2, Surface Pro 3, Surface Pro 2, Surface Pro, Surface 2, Surface, Windows RT 8.1, Windows Phone 8.1, Windows Embedded 8.1 Industry Enterprise, StorSimple 8000 Series, Azure StorSimple Virtual Array Windows Server 2012 R2  \* 3651 - Secure Kernel Code Integrity  \* 3644 - Code Integrity  \* 3615 - Windows OS Loader  \* 3197 - Cryptographic Primitives Library  \* 3196 - Kernel Mode Cryptographic Primitives Library  \* 3092 - BitLocker Dump Filter  \* 3089 - Boot Manager  The Linux servers employ NIST-certified Federal Information Processing Standards (FIPS) 140-2 compliant cryptographic modules.  \* 3647 - Ubuntu 18.04 Kernel Crypto API Cryptographic Module  \* 3622 - Ubuntu 18.04 OpenSSL Cryptographic Module  \* 3633 - Ubuntu 18.04 OpenSSH Client Cryptographic Module  \* 3632 - Ubuntu 18.04 OpenSSH Server Cryptographic Module  \* 3648 - Ubuntu 18.04 Strongswan Cryptographic Module  \* 3683 - Ubuntu 18.04 Azure Kernel Crypto API Cryptographic Module  \* 2962 - Ubuntu Kernel Crypto API Cryptographic Module  \* 2888 - Ubuntu OpenSSL Cryptographic Module  \* 2907 - Ubuntu OpenSSH Client Cryptographic Module  \* 2906 - Ubuntu OpenSSH Server Cryptographic Module  \* 2978 - Ubuntu Strongswan Cryptographic Module  \* 4277 - Microsoft Azure Linux Kernel Crypto API (Formerly CBL-Mariner 1.0 Kernel Crypto API)  \* 4496 - Microsoft Azure Linux OpenSSL Cryptographic Library (Formerly CBL-Mariner 2.0 OpenSSL Cryptographic Module)  \* 4292 - Ubuntu 20.04 OpenSSL Cryptographic Module  \* 4126 - Ubuntu 20.04 Azure Kernel Crypto API Cryptographic Module  \* 4046 - Ubuntu 20.04 Strongswan Cryptographic Module  \* 3966 - Ubuntu 20.04 OpenSSL Cryptographic Module  \* 3928 - Ubuntu 20.04 Kernel Crypto API Cryptographic Module"  \* 3902 - Ubuntu 20.04 Libgcrypt Cryptographic Module  \* 3939 - Red Hat Enterprise Linux 7 Kernel Crypto API Cryptographic Module"  \* 3725 - Ubuntu 16.04 OpenSSL Cryptographic Module"  \* 3724 - Ubuntu 16.04 Kernel Crypto API Cryptographic Module  \* 3980 - Ubuntu 18.04 OpenSSL Cryptographic Module  \* 3876 - Red Hat Enterprise Linux 7 OpenSSL Cryptographic Module"  \* 3538 - Red Hat Enterprise Linux OpenSSL Cryptographic Module"  \* 3016 - Red Hat Enterprise Linux OpenSSL Cryptographic Module"  \* 4642 - Red Hat Enterprise Linux 8 OpenSSL Cryptographic Module  \* 4458 - Red Hat Enterprise Linux 8 NSS Cryptographic Module  \* 4438 - Red Hat Enterprise Linux 8 libgcrypt Cryptographic Module  \* 4434 - Red Hat Enterprise Linux 8 Kernel Crypto API Cryptographic Module  \* 4428 - Red Hat Enterprise Linux 8 GnuTLS Cryptographic Module  \* 4413 - Red Hat Enterprise Linux 8 NSS Cryptographic Module  \* 4397- Red Hat Enterprise Linux 8 libgcrypt Cryptographic Module  \* 4384 - Red Hat Enterprise Linux 8 libgcrypt Cryptographic Module  \* 4272 - Red Hat Enterprise Linux 8 GnuTLS Cryptographic Module  \* 4271 - Red Hat Enterprise Linux 8 OpenSSL Cryptographic Module  \* 4254 - Red Hat Enterprise Linux 8 Kernel Crypto API Cryptographic Module  \* 3784 - Red Hat Enterprise Linux 8 libgcrypt Cryptographic Module  \* 3956 - Red Hat Enterprise Linux 8 GnuTLS Cryptographic Module  \* 3946 - Red Hat Enterprise Linux 8 NSS Cryptographic Module  \* 3918 - Red Hat Enterprise Linux 8 Kernel Crypto API Cryptographic Module  \* 3842 - Red Hat Enterprise Linux 8 OpenSSL Cryptographic Module  \* 3839 - Red Hat Enterprise Linux 8 NSS Cryptographic Module  \* 3813 - Red Hat Enterprise Linux 8 GnuTLS Cryptographic Module  \* 3794 - Red Hat Enterprise Linux 8 Kernel Crypto API Cryptographic Module  \* 3781 - Red Hat Enterprise Linux 8 OpenSSL Cryptographic Module  \* 3892 - Red Hat Enterprise Linux 7 OpenSSH Client Cryptographic Module  \* 3891 - Red Hat Enterprise Linux 7 OpenSSH Server Cryptographic Module  \* 3867 - Red Hat Enterprise Linux 7 OpenSSL Cryptographic Module  \* 3860 - Red Hat Enterprise Linux 7 NSS Cryptographic Module  \* 3563 - Red Hat Enterprise Linux 7 Libreswan Cryptographic Module  \* 2441 - Red Hat Enterprise Linux 6.6 OpenSSL Module, Red Hat Enterprise Linux 7.1 OpenSSL Module  \* 4498 - Red Hat Enterprise Linux 7 NSS Cryptographic Module  \* 4282 - OpenSSL FIPS Provider  **Network Devices**  Encrypted data may transit across the Azure network, but the network devices are agnostic as to the type of data being transmitted. Network devices use the following cryptographic modules:  \* 2984 - Cisco FIPS Object Module  \* 2505 - Cisco FIPS Object Module  \* 3429 - EOS MACsec Alpha Hybrid Module  \* 3420 - EOS MACsec Bravo Hybrid Module  \* 2909 - Arista EOS Crypto Module v1.0  \* 3621 - Juniper Networks MX80, MX104, MX240, MX480, MX960 3D Universal Edge Routers with RE-S-X6-64G/RE-S-X6-128G Routing Engine and MIC-MACSEC-20GE MACSec Card  \* 2921 - Juniper Networks SRX1400, SRX3400, and SRX3600 Services Gateways  \* 3629 - F5® Device Cryptographic Module  \* 2988 - Citrix FIPS Cryptographic Module  \* 4019 - Arista EOS Crypto Module  \* 1521 - Cisco 2951, Cisco 3925 and Cisco 3945 Integrated Services Routers (ISRs)  \* 2409 - Cisco ASR 1001, 1001-X, 1002, 1002-X, 1004, 1006 and 1013  \* 2090 - Cisco ASR 1001, ASR 1002, ASR1002-X, ASR 1004, ASR 1006 and ASR 1013  \* 3775 - Cisco ASR 1000 Series Routers with MACSEC  \* 3988 - Cisco ASR 1000 Series Routers without MACSEC  \* 3841 - F5® Device Cryptographic Module  \* 2896 - Pulse Secure Cryptographic Module  \* 3416 - Juniper Networks MX240, MX480, MX960, MX2010, MX2020 3D Universal Edge Routers and EX9204, EX9208, EX9214 Ethernet Switches with RE1800 Routing Engine  \* 3934 - Juniper Networks MX240, MX480, MX960 3D Universal Edge Routers with RE1800 Routing Engine and Multiservices MPC  \* 3935 - Juniper Networks MX240, MX480, MX960 3D Universal Edge Routers with RE1800 Routing Engine and MPC7E-10G MACsec Card  \* 2388 - IOS Common Cryptographic Module (IC2M) Rel5  AES-256 bit encrypted SSH is used for network device authentication using Federal Information Processing Standards (FIPS) 140-2 approved algorithms:  \* 0048 - SecureCRT VanDyke 8.0.3 (FIPS Validation Certificate 0048)  \* 2643 - nShield F2 500+, nShield F2 1500+ and nShield F2 6000+  **Azure Key Stores**  The Thales nShield Hardware Security Modules used by KeyVault employ cryptographic modules certified by NIST as being Federal Information Processing Standards (FIPS) 140-2 compliant; relevant NIST certificate number is 2643. Azure Managed HSM and KeyVault utilize CMVP certificate number 4399 from Marvell vendor. Azure Dedicated HSM utilizes CMVP certificate numbers 4090 and 4684 certificate numbers from Thales vendor. Azure leverages the NIST CMVP certificate numbers 3517, 3914, and 3907 for Yubico, Inc. cryptographic modules to enable multi-factor authentication within Azure cloud production environments.  Azure has an alternative implementation for the security control. Azure baseline configurations tracked via AzSecPack are designed to implement and monitor appropriate ciphers used for authentication. Moreover, Azure implements Federal Information Processing Standards (FIPS) 140-2-approved algorithms in CMVP-validated cryptographic modules but is currently unable to run all servers in FIPS mode. Where possible, Azure implements FIPS mode on servers. However, FIPS mode has operational impacts on key Azure services for non-security cryptographic implementations. In addition, some cipher suites which are considered weak are used to accommodate Azure customers. Lastly, Microsoft continues to drive TLS 1.2 and 1.3 only within Azure. Elimination of TLS 1.0 and 1.1 is an Enterprise Promise, ensuring visibility at the highest levels of Azure Asset misconfigurations do occur, but are monitored and tracked via AzSecPack baseline settings. If an asset allows TLS 1.0 or 1.1, the owning service team is alerted via monitoring tools. Azure uses multiple reporting engines to ensure all TLS below 1.2 and 1.3 is identified and appropriate action is taken. It’s important to note some externally facing services must support older TLS versions for customer purposes. |

## SC-15 Collaborative Computing Devices and Applications

a. Prohibit remote activation of collaborative computing devices and applications with the following exceptions: [no exceptions for computing devices] ; and

b. Provide an explicit indication of use to users physically present at the devices.

Requirement: The information system provides disablement (instead of physical disconnect) of collaborative computing devices in a manner that supports ease of use.

|  |
| --- |
| **SC-15 Control Summary Information** |
| Responsible Roles: Azure Compliance |
| Parameter sc-15(a): no exceptions for computing devices |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☒ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☒ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SC-15 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for prohibiting remote activation of any collaborative computing devices within or controlled from customer-deployed resources and defining exceptions where remote activation is allowed (if any).  **Azure**  Azure does not allow collaborative computing devices and there are no instances of collaborative computing devices within the Azure accreditation boundary managed by Azure. This includes Hyper-V clipboard functions, microphones, network white boards, and cameras. |
| **Part B**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for providing a notification when physically presenting at a collaborative device.  **Azure**  Azure does not allow collaborative computing devices and there are no instances of collaborative computing devices within the Azure accreditation boundary managed by Azure. This includes Hyper-V clipboard functions, microphones, network white boards, and cameras. |

## SC-17 Public Key Infrastructure Certificates

a. Issue public key certificates under an [a certificate policy for issuing public key certificates is defined;] or obtain public key certificates from an approved service provider; and

b. Include only approved trust anchors in trust stores or certificate stores managed by the organization.

|  |
| --- |
| **SC-17 Control Summary Information** |
| Responsible Roles: Secret Management Stores |
| Parameter sc-17(a): Public Key Infrastructure Operational Security Standard |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SC-17 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for defining and enforcing a policy for issuing public key certificates or obtaining public key certificates from an approved service provider.  Government customers are responsible for having a process in place to check the validity of the Azure websites prior to signing on by reviewing the digital certificate on the site to ensure they are the Azure websites. If government customers are using USGCB baselines, supported web browsers will enforce this review automatically by default and prevent connections if the digital certificate is invalid.  **Azure**  The Key Management Standard applies to the operation of all Microsoft’s online services residing within the Azure environment utilizing cryptographic mechanisms for securing data or services. This standard applies to all environments managed by Azure, including labs, production, and preproduction.  Microsoft’s corporate Public Key Infrastructure (PKI) has been established to provide a variety of digital certificate services to support operations for Azure and for the Microsoft Corporation. Microsoft corporate PKI functions as the Certificate Authority (CA) and Registration Authority (RA) and provides directory services to manage keys and certificates. Internal Azure traffic does not require the use of digital certificates and also includes the use of self-signed certificates. The use of self-signed certificates applies exclusively to internal use within Azure. |
| **Part B**  **Customer Responsibility**  The customer is responsible to only include approved trust anchors in trust stores or certificate stores managed for customer-deployed resources.  **Azure**  The Key Management Standard applies to the operation of all Microsoft’s online services residing within the Azure environment utilizing cryptographic mechanisms for securing data or services. This standard applies to all environments managed by Azure, including labs, production, and preproduction.  Microsoft’s corporate Public Key Infrastructure (PKI) has been established to provide a variety of digital certificate services to support operations for Azure and for the Microsoft Corporation. Microsoft corporate PKI functions as the Certificate Authority (CA) and Registration Authority (RA) and provides directory services to manage keys and certificates. Internal Azure traffic does not require the use of digital certificates and also includes the use of self-signed certificates. The use of self-signed certificates applies exclusively to internal use within Azure. |

## SC-18 Mobile Code

a. Define acceptable and unacceptable mobile code and mobile code technologies; and

b. Authorize, monitor, and control the use of mobile code within the system.

|  |
| --- |
| **SC-18 Control Summary Information** |
| Responsible Roles: SDL |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SC-18 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for defining acceptable and unacceptable mobile code technologies.  **Azure**  Microsoft’s Security Development Lifecycle (SDL) process includes provisions for defining acceptable and unacceptable mobile code technologies. Unapproved mobile code is any mobile code that has not been developed and approved through the SDL. |
| **Part B**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for authorizing, monitoring, and controlling the use of mobile code within customer-deployed resources.  **Azure**  Azure authorizes, monitors, and controls the use of mobile code developed by the service teams using the SDL, including peer review and the Security Code Review, to detect the presence of unauthorized mobile code. Code may not be released without following SDL processes. |

## SC-20 Secure Name/Address Resolution Service (Authoritative Source)

a. Provide additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and

b. Provide the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

Requirement: Control Description should include how DNSSEC is implemented on authoritative DNS servers to supply valid responses to external DNSSEC requests.

Requirement: Authoritative DNS servers must be geolocated in accordance with SA-9 (5).

Guidance: SC-20 applies to use of external authoritative DNS to access a CSO from outside the boundary.

Guidance: External authoritative DNS servers may be located outside an authorized environment. Positioning these servers inside an authorized boundary is encouraged.

Guidance: CSPs are recommended to self-check DNSSEC configuration through one of many available analyzers such as Sandia National Labs (https://dnsviz.net)

|  |
| --- |
| **SC-20 Control Summary Information** |
| Responsible Roles: Networking |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☒ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SC-20 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for a secure name and address resolution service, including providing data origin authentication and integrity verification as well as authoritative name resolution data in response to name and address resolution queries. Note: this control is only applicable to the customer if hosting DNS and resolving .gov domains.  Azure does not currently support DNSSEC; however, there is a plan to implement this feature within an estimated timeframe of two years. The absence of DNSSEC in Azure does not pose a significant security risk, as all Azure services utilize HTTPS/TLS rather than plain HTTP. TLS provides both authentication and encryption, ensuring that clients connect to trusted servers and that communication between clients and servers is secure. Even in scenarios where clients detect a tampered DNS response and connect to a server controlled by a bad actor, TLS offers protection. TLS requires servers to present a valid cryptographic certificate to clients, establishing the server's identity. If the client cannot verify the server's identity based on the presented certificates, it can terminate the connection. This effectively mitigates any security concerns that could arise from the lack of DNSSEC. It is not mandatory for Azure customers to use Azure's DNS hosting service. If DNSSEC is a critical requirement, customers have the option to host DNS Zones with third-party DNS hosting providers that support DNSSEC or to host the zones on their own DNS servers running on Azure VMs. Additionally, customers are not required to use Azure's provided recursive resolvers for resolving DNS queries from Azure virtual networks. Azure allows customers to deploy their own VM-based DNS servers within virtual networks. These servers can be configured to support DNSSEC validation and verification, and customers can use them to resolve DNS queries instead of Azure's provided recursive resolvers.  **Azure**  The Azure DNS infrastructure provides internal name resolution for internal Microsoft assets and external name resolution services to external customers, including Federal Agencies. However, Azure does not support DNSSEC and a customer is required to either bring their own DNS servers into Azure or use a third-party DNS provider if DNSSEC is a requirement. Azure uses three types of DNS servers.  Azure DNS servers act as non-authoritative sources for DNS requests only from clients hosted inside Azure. A client makes a DNS query to a system DNS server; the system DNS server in turn queries an authoritative source outside the system. System DNS servers do not support the DNSSEC protocol. This control requires system DNS servers, when requested by clients, to perform origin/integrity verification of the response provided by authoritative sources. The control assumes that the client makes a DNS query of a system DNS server and that the DNS server must then query an authoritative source outside the system. The risk that the external authoritative source has been compromised is mitigated by the origin/integrity verification.  Azure internal DNS servers resolve DNS queries from Azure servers. Azure servers do not request origin/integrity verification of the DNS query; instead origin/integrity is assured via other means such as the communications channel using TLS.  Azure DNS production servers act as authoritative sources for DNS requests from external clients for various Azure domains and do not respond to any DNS queries against zones for which they are not the authority.  This control requires system DNS servers, when requested by clients, to perform origin/integrity verification of the response provided by authoritative sources. The control assumes that the client makes a DNS query of a system DNS server and that the DNS server must then query an authoritative source outside the system. The risk that the external authoritative source has been compromised is mitigated by the origin/integrity verification. Azure DNS servers perform two functions:  1. Resolving DNS queries from Azure servers.  2. Acting as authoritative sources for DNS requests from external clients for certain Microsoft.com subdomains.  For case 1, queries are either for internal domains for which Azure DNS servers are authoritative, or for external domains used by Azure’s services. In either case, Azure servers do not request origin/integrity verification of the DNS query. For case 2, this case is not possible for Azure DNS servers. |
| **Part B**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for a secure name and address resolution service, including the ability to provide the security status of child zones in order to verify chain of trust among parent and child domains. Note: this control is only applicable to the customer if hosting DNS and resolving .gov domains.  Azure does not currently support DNSSEC; however, there is a plan to implement this feature within an estimated timeframe of two years. The absence of DNSSEC in Azure does not pose a significant security risk, as all Azure services utilize HTTPS/TLS rather than plain HTTP. TLS provides both authentication and encryption, ensuring that clients connect to trusted servers and that communication between clients and servers is secure. Even in scenarios where clients detect a tampered DNS response and connect to a server controlled by a bad actor, TLS offers protection. TLS requires servers to present a valid cryptographic certificate to clients, establishing the server's identity. If the client cannot verify the server's identity based on the presented certificates, it can terminate the connection. This effectively mitigates any security concerns that could arise from the lack of DNSSEC. It is not mandatory for Azure customers to use Azure's DNS hosting service. If DNSSEC is a critical requirement, customers have the option to host DNS Zones with third-party DNS hosting providers that support DNSSEC or to host the zones on their own DNS servers running on Azure VMs. Additionally, customers are not required to use Azure's provided recursive resolvers for resolving DNS queries from Azure virtual networks. Azure allows customers to deploy their own VM-based DNS servers within virtual networks. These servers can be configured to support DNSSEC validation and verification, and customers can use them to resolve DNS queries instead of Azure's provided recursive resolvers.  **Azure**  The Azure DNS infrastructure provides internal name resolution for internal Microsoft assets and external name resolution services to external customers, including Federal Agencies. However, Azure does not support DNSSEC and a customer is required to either bring their own DNS servers into Azure or use a third-party DNS provider if DNSSEC is a requirement.  Azure DNS is a public service and anyone from internet can access externally hosted zones. For internal Azure services that depend on DNS, Microsoft employs TLS to mitigate the need for DNSSEC. Azure customers who intend to secure their applications against DNS-based attacks can also use TLS to mitigate the need for DNSSEC.  Microsoft implements compensating controls that mitigate the risk of not enacting DNSSEC according to IPSEC policy. HTTPS/TLS is required for all connections into the Azure environment, establishing secure connections with Azure resources. A customer connecting to an invalid server still needs to be presented with a valid certificate to risk a security breach. Because the TLS/HTTPS implementation provides both authentication and encryption, Microsoft considers it sufficient for mitigating the risks of internal servers not being configured with DNSSEC. Outside of the effectiveness of TLS/HTTPS, customers can deploy their own VM-based DNS servers in the virtual networks. Customers can also choose to host DNS Zones with third-party DNS hosting providers that support DNSSEC. Customers can also configure their own DNS servers to support DNSSEC validation/verification and use these servers to resolve DNS queries instead of Azure provided recursive resolver. |

## SC-21 Secure Name/Address Resolution Service (Recursive or Caching Resolver)

Request and perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

Requirement: Control description should include how DNSSEC is implemented on recursive DNS servers to make DNSSEC requests when resolving DNS requests from internal components to domains external to the CSO boundary. \* If the reply is signed, and fails DNSSEC, do not use the reply \* If the reply is unsigned: \* CSP chooses the policy to apply

Requirement: Internal recursive DNS servers must be located inside an authorized environment. It is typically within the boundary, or leveraged from an underlying IaaS/PaaS.

Guidance: Accepting an unsigned reply is acceptable

Guidance: SC-21 applies to use of internal recursive DNS to access a domain outside the boundary by a component inside the boundary. - DNSSEC resolution to access a component inside the boundary is excluded.

|  |
| --- |
| **SC-21 Control Summary Information** |
| Responsible Roles: Networking |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☒ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SC-21 What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for configuring customer-deployed resources to request and perform data origin authentication and data integrity verification on name/address resolution responses received from authoritative sources.  Azure does not currently support DNSSEC; however, there is a plan to implement this feature within an estimated timeframe of two years. The absence of DNSSEC in Azure does not pose a significant security risk, as all Azure services utilize HTTPS/TLS rather than plain HTTP. TLS provides both authentication and encryption, ensuring that clients connect to trusted servers and that communication between clients and servers is secure. Even in scenarios where clients detect a tampered DNS response and connect to a server controlled by a bad actor, TLS offers protection. TLS requires servers to present a valid cryptographic certificate to clients, establishing the server's identity. If the client cannot verify the server's identity based on the presented certificates, it can terminate the connection. This effectively mitigates any security concerns that could arise from the lack of DNSSEC. It is not mandatory for Azure customers to use Azure's DNS hosting service. If DNSSEC is a critical requirement, customers have the option to host DNS Zones with third-party DNS hosting providers that support DNSSEC or to host the zones on their own DNS servers running on Azure VMs. Additionally, customers are not required to use Azure's provided recursive resolvers for resolving DNS queries from Azure virtual networks. Azure allows customers to deploy their own VM-based DNS servers within virtual networks. These servers can be configured to support DNSSEC validation and verification, and customers can use them to resolve DNS queries instead of Azure's provided recursive resolvers.  **Azure**  Azure DNS resolvers do not support DNSSEC and hence do not verify the integrity of a DNS response. Customers who require DNSSEC are required to bring their own DNS resolver servers.  Microsoft implements compensating controls that mitigate the risk of not enacting DNSSEC according to IPSEC policy. HTTPS/TLS is required for all connections into the Azure environment, establishing secure connections with Azure resources. A customer connecting to an invalid server still needs to be presented with a valid certificate to risk a security breach. Because the TLS/HTTPS implementation provides both authentication and encryption, Microsoft considers it sufficient for mitigating the risks of internal servers not being configured with DNSSEC. Outside of the effectiveness of TLS/HTTPS, customers can deploy their own VM-based DNS servers in the virtual networks. Customers can also choose to host DNS Zones with third-party DNS hosting providers that support DNSSEC. Customers can also configure their own DNS servers to support DNSSEC validation/verification and use these servers to resolve DNS queries instead of Azure provided recursive resolver. |

## SC-22 Architecture and Provisioning for Name/Address Resolution Service

Ensure the systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal and external role separation.

|  |
| --- |
| **SC-22 Control Summary Information** |
| Responsible Roles: Networking |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SC-22 What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for ensuring that the systems providing address resolution services for customer-deployed resources are fault-tolerant and implement internal/external role separation. Note: if customers configure their Domain Name Server (DNS) settings to use Azure servers, Azure DNS can support fault tolerance.  **Azure**  The Azure DNS offering provides name and address resolution. Fault tolerance is built into the service through redundancy at multiple levels, including multiple DNS server clusters and multiple servers per cluster, and deployment at multiple Azure datacenter facilities which are geographically separated. Azure DNS also leverages network controls to restrict type of hosts that can access an authoritative DNS server in a particular role.  The implementation incorporates a master repository of DNS zones. Master repository is deployed in multiple datacenters across different geographical regions for redundancy purposes. Data from master repository is pulled into edge DNS servers on demand for resolving authoritative DNS queries. Data from master repository is backed up and monitored with the security incident and event management tool as documented in the AU family of controls.  Additionally, a backup system built using a completely different hardware and software system stack is implemented and kept in sync with the master repository. This system is engaged in case of a catastrophic failure of the primary system.  Azure DNS recursive resolver service has built-in cross region failover capability that automatically switches the DNS traffic to another region in case there is a catastrophic failure of DNS resolution in one region. |

## SC-23 Session Authenticity

Protect the authenticity of communications sessions.

|  |
| --- |
| **SC-23 Control Summary Information** |
| Responsible Roles: Networking |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SC-23 What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for protecting the authenticity of communications sessions involving customer-deployed resources. Customers are responsible for having a process in place to check the validity of the Azure websites prior to signing on by reviewing the digital certificate on the site to ensure they are the Azure websites. If customers are using USGCB baselines, supported web browsers enforce this review automatically by default and prevent connections if the digital certificate is invalid.  **Azure**  Azure uses digital certificates to establish the identity of Jumpboxes, Debug servers, and Network Hop Boxes as the access points to the Azure environment. Digital certificates are used in public key cryptography (PKI) to establish the identity of assets for purposes of authentication. This also supports encrypted connections using TLS, which is resistant to person-in-the-middle attacks.  All communications between Azure internal components that transfer confidential information are protected using TLS. In most cases, SSL certificates are self-signed, and their fingerprints are distributed over the same channels as the IP addresses. Exceptions are for any certificates for connections that could be accessed from outside the Azure network, including the storage service, and for the Fabric Controllers (FCs). FCs have certificates issued by a Microsoft Certificate Authority (CA) that chains back to a trusted root CA. |

## SC-24 Fail in Known State

Fail to a [known system state to which system components fail in the event of a system failure is defined;] for the following failures on the indicated components while preserving [system state information to be preserved in the event of a system failure is defined;] in failure: [types of system failures for which the system components fail to a known state are defined;].

|  |
| --- |
| **SC-24 Control Summary Information** |
| Responsible Roles: BCDR |
| Parameter sc-24\_odp.01: operational failure of boundary protection devices, load balancers, or dedicated network devices |
| Parameter sc-24\_odp.02: secure, closed state |
| Parameter sc-24\_odp.03: all data within the system |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SC-24 What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for ensuring that customer-deployed resources fail in a known-state for customer-defined types of failures to preserve the system state information in failure.  **Azure**  To preserve data in the event of a system failure, Azure implements geographic redundancy and data mirroring. Azure employs geo-replication for Azure assets which can establish alternate storage sites geographically. Synchronization is the process of ensuring that files and directories already exist on the replica server and that they are identical to the original copies on the master server. Synchronization occurs before replication. Furthermore, Azure databases are data replicated through live mirroring.  Boundary protection devices fail over to equally secure backup devices. In the event the process fails, the mechanisms fail to a known secure closed state, preserving confidentiality and integrity of all data within the system. |

## SC-28 Protection of Information at Rest

Protect the [Selection (OneOrMore): confidentiality;integrity] of the following information at rest: [information at rest requiring protection is defined;].

Guidance: The organization supports the capability to use cryptographic mechanisms to protect information at rest.

Guidance: When leveraging encryption from underlying IaaS/PaaS: While some IaaS/PaaS services provide encryption by default, many require encryption to be configured, and enabled by the customer. The CSP has the responsibility to verify encryption is properly configured.

Guidance: Note that this enhancement requires the use of cryptography in accordance with SC-13.

|  |
| --- |
| **SC-28 Control Summary Information** |
| Responsible Roles: Storage |
| Parameter sc-28\_odp.01: confidentiality and integrity |
| Parameter sc-28\_odp.02: customer data |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SC-28 What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for protecting customer-controlled information at rest. Azure Storage provides the capability for customers to protect their information at rest using Azure SAKs provided by Azure. The SAK is a secret key that is used to manage access to storage. An application that needs to access storage must have possession of this key. It is the customer’s responsibility to protect the SAKs in order to protect their data.  **Azure**  Azure protects information at rest by applying information-handling procedures. Assets must be protected per the standards appropriate for their defined asset class. Microsoft’s Online Services has devised a set of minimum required protection standards for each asset class to appropriately protect the confidentiality, integrity, and availability of each asset. These minimum standards are defined in the Asset Classification Standard and Asset Protection Standard. Data must be classified according to Corporate, External, and Legal Affairs (CELA) data classifications and associated retentions. Protections for information at rest are outlined in, but not limited to, the categories below:  \* Azure Storage automatically encrypts data when persisting it to the cloud. Data in Azure Storage is encrypted and decrypted transparently using 256-bit AES encryption, one of the strongest block ciphers available, and is Federal Information Processing Standards (FIPS) 140-2 compliant. Azure Storage encryption is enabled for all new and existing storage accounts and cannot be disabled. Storage accounts are encrypted regardless of their performance tier (standard or premium) or deployment model (Azure Resource Manager or classic). All Azure Storage redundancy options support encryption, and all copies of a storage account are encrypted. All Azure Storage resources are encrypted, including blobs, disks, files, queues, and tables. All object metadata is also encrypted.  \* For each block written to Azure Storage accounts, a compressed and uncompressed CRC is used to identify corrupted data. Azure Storage checks the CRC after every major handoff of the data. In addition, a background job periodically runs on the extant assets checking the data checksum to find corrupted data.  \* Azure uses the Transport Layer Security (TLS) protocol to protect data traveling between Azure services and customers. Azure datacenters negotiate a TLS connection with client systems that connect to Azure services. Perfect Forward Secrecy (PFS) protects connections between customers’ client systems and Azure services by unique keys. Connections also use RSA-based 2,048-bit encryption key lengths.  \* Logical access to protected data at rest is controlled at various levels through technical means. Access to servers where information is stored is restricted through Active Directory security group membership in the domain where the server resides. Security groups that restrict access to information at rest are configured to allow the least privilege possible to complete tasks. Any Microsoft personnel needing access must follow account creation, modification, and escalation procedures.  \* Technical means also create logical access control at the network layer. ACLs prevent servers that store data at rest from being exposed outside of the environment.  \* The Azure datacenter teams maintain controls over physical access. The server rooms and caged environments have multiple access levels regulated with least privilege.  \* Privileged Access Workstation (PAWs) utilizes BitLocker to protect information at rest. |

### SC-28(1) - Cryptographic Protection

Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [all information system components storing Federal data or system data that must be protected at the High or Moderate impact levels]: [information requiring cryptographic protection is defined;].

Guidance: Organizations should select a mode of protection that is targeted towards the relevant threat scenarios. Examples: A. Organizations may apply full disk encryption (FDE) to a mobile device where the primary threat is loss of the device while storage is locked. B. For a database application housing data for a single customer, encryption at the file system level would often provide more protection than FDE against the more likely threat of an intruder on the operating system accessing the storage. C. For a database application housing data for multiple customers, encryption with unique keys for each customer at the database record level may be more appropriate.

|  |
| --- |
| **SC-28(1) Control Summary Information** |
| Responsible Roles: Storage |
| Parameter sc-28.01\_odp.01: customer data |
| Parameter sc-28.01\_odp.02: Azure servers |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SC-28(1) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for protecting customer-controlled information at rest from unauthorized disclosure and modification.  **Azure**  Azure Storage automatically encrypts data when persisting it to the cloud. Data in Azure Storage is encrypted and decrypted transparently using 256-bit AES encryption, one of the strongest block ciphers available, and is Federal Information Processing Standards (FIPS) 140-2 compliant. Azure Storage encryption is enabled for all new and existing storage accounts and cannot be disabled. Storage accounts are encrypted regardless of their performance tier (standard or premium) or deployment model (Azure Resource Manager or classic). All Azure Storage redundancy options support encryption, and all copies of a storage account are encrypted. All Azure Storage resources are encrypted, including blobs, disks, files, queues, and tables. All object metadata is also encrypted. |

## SC-39 Process Isolation

Maintain a separate execution domain for each executing system process.

|  |
| --- |
| **SC-39 Control Summary Information** |
| Responsible Roles: Azure Compliance |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SC-39 What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for maintaining separate execution domains for running processes.  **Azure**  All Azure servers run operating systems that maintain separate execution domains for each executing process by assigning a private virtual address space to each process. In addition, all operating systems used in the Azure environment employ multi-thread processing, which is consistent with modern operating systems. Multi-thread processing allows for multiple processes to be executed concurrently and in isolation. See the following TechNet article for more information:  <https://docs.microsoft.com/en-us/windows/win32/memory/memory-protection>. |

## SC-45 System Time Synchronization

Synchronize system clocks within and between systems and system components.

|  |
| --- |
| **SC-45 Control Summary Information** |
| Responsible Roles: Logging and Monitoring, Networking, Compute |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SC-45 What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for synchronizing system clocks within and between customer-deployed resources.  **Azure**  For Bare Metal servers, all assets are joined to an Active Directory domain and configured to receive authenticated time updates from the local domain controller via NTP and synchronize at least hourly. For Azure-based servers and network devices, all assets are configured to use the Coordinated Universal Time (UTC) setting when generating event logs. Once servers are joined to an Active Directory domain, they are configured by policy to receive authenticated time updates from the local domain controller via NTP and synchronize at least hourly and update the time if it is off by 1 millisecond or more. Local domain controllers obtain their time updates from Azure time servers. All Azure servers are configured to synchronize every five (5) minutes through Azure-managed domain controllers; network devices synchronize every five (5) minutes with the same time servers used by the Azure domain controllers. The Azure time servers are NTP stratum 1 time servers. Azure manages two different NTP time servers in separate geographic locations. The time servers are geographically dispersed and located in multiple separate Azure-managed datacenters. Azure chooses to use the GPS satellites as the authoritative time source as an alternative to the NIST time hosts.  All Azure assets synchronize the internal system clocks to the authoritative time source at least every hour and update the time if it is off by one (1) millisecond or more. |

### SC-45(1) - Synchronization with Authoritative Time Source

(a) Compare the internal system clocks [At least hourly] with [http://tf.nist.gov/tf-cgi/servers.cgi] ; and

(b) Synchronize the internal system clocks to the authoritative time source when the time difference is greater than [any difference].

Requirement: The service provider selects primary and secondary time servers used by the NIST Internet time service. The secondary server is selected from a different geographic region than the primary server.

Requirement: The service provider synchronizes the system clocks of network computers that run operating systems other than Windows to the Windows Server Domain Controller emulator or to the same time source for that server.

Guidance: Synchronization of system clocks improves the accuracy of log analysis.

|  |
| --- |
| **SC-45(1) Control Summary Information** |
| Responsible Roles: Logging and Monitoring, Networking, Compute |
| Parameter sc-45.01\_odp.01: organization-defined frequency |
| Parameter sc-45.01\_odp.02: organization-defined authoritative time source |
| Parameter sc-45.01\_odp.03: organization-defined time period |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SC-45(1) What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  The customer is responsible for comparing internal system clocks at a defined frequency with defined authoritative time source for customer-deployed resources.  **Azure**  Azure manages two different NTP time servers in separate geographic locations. The time servers are geographically dispersed and located in multiple separate Azure-managed datacenters. Azure chooses to use the GPS satellites as the authoritative time source as an alternative to the NIST time hosts. Azure compares internal system clocks deployed on Azure assets to GPS satellites. All Azure assets synchronize the internal system clocks to the authoritative time sources at least every hour and update the time if it is off by one (1) millisecond or more. |
| **Part B**  **Customer Responsibility**  The customer is responsible for synchronizing the internal system clocks to the authoritative time source when the time difference is greater than defined time period for customer-deployed resources.  **Azure**  Azure manages two different NTP time servers in separate geographic locations. The time servers are geographically dispersed and located in multiple separate Azure-managed datacenters. Azure chooses to use the GPS satellites as the authoritative time source as an alternative to the NIST time hosts. Azure synchronizes internal system clocks deployed on Azure assets to GPS satellites. All Azure assets synchronize the internal system clocks to the authoritative time sources at least every hour and update the time if it is off by one (1) millisecond or more. |

# System and Information Integrity (SI)

## SI-1 Policy and Procedures

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

1. [Selection (OneOrMore): organization-level;mission/business process-level;system-level] system and information integrity policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the system and information integrity policy and the associated system and information integrity controls;

b. Designate an [an official to manage the system and information integrity policy and procedures is defined;] to manage the development, documentation, and dissemination of the system and information integrity policy and procedures; and

c. Review and update the current system and information integrity:

1. Policy [at least annually] and following [events that would require the current system and information integrity policy to be reviewed and updated are defined;] ; and

2. Procedures [at least annually] and following [significant changes].

|  |
| --- |
| **SI-1 Control Summary Information** |
| Responsible Roles: SOP Team, Policy |
| Parameter si-1(a): all personnel |
| Parameter si-01\_odp.01: |
| Parameter si-01\_odp.02: |
| Parameter si-01\_odp.03: a Microsoft-wide |
| Parameter si-01\_odp.04: the Microsoft Information Risk Management Council (IRMC) organization |
| Parameter si-01\_odp.05: at least annually |
| Parameter si-01\_odp.06: significant changes |
| Parameter si-01\_odp.07: at least annually |
| Parameter si-01\_odp.08: significant changes |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☒ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SI-1 What is the solution and how is it implemented?** |
| **Part A1**  **Customer Responsibility**  The customer is responsible for developing, documenting, and disseminating system and information integrity policy and procedures that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.  **Azure**  Azure addresses the system and information integrity policy as part of the Microsoft security policies, of which there are two sets: the Microsoft Security Policy (MSP) that is applicable to all Microsoft personnel, and the Microsoft Security Program Policy (MSPP), which is applicable to all Microsoft personnel that have a responsibility for security. The Microsoft Information Risk Management Council (IRMC) is the governance body with review and approval responsibility for the MSP and MSPP. Within Azure, the MSPP specifically applies to all Microsoft personnel with security objectives such as designing, building, and operating Azure and across all information and processes used in the conduct of Microsoft business. All Azure personnel are accountable and responsible for complying with these guiding principles within their designated roles. The policy addresses the following:  \* Asset handling  \* Logging and monitoring  Additionally, the policy addresses the purpose, scope, roles, responsibilities, compliance requirements, and required coordination among the various Microsoft organizations that provide some level of support to all services. The policies indicate Microsoft management’s commitment and are a component of the risk management strategy which provides Azure personnel with a current set of clear and concise information security requirements.  The MSP is available to all Microsoft personnel on the Microsoft Policy website on the Microsoft intranet, and the MSPP and Security Standards are available through the Liquid tool, also on the Microsoft intranet. The Azure SOPs are stored in the Azure Security, Privacy & Compliance SharePoint site. This SharePoint site is accessible to all Azure personnel.  Service teams may supplement the Azure policies and procedures with offering-specific policies and procedures. Service-team-specific policies and procedures associated with access control are documented and stored within internal Azure SharePoint sites. Only personnel with authorized credentials, adequate levels of permission, legitimate need to know, and specific roles and responsibilities are given access to the service-team-specific policies or procedures. |
| **Part A2**  **Customer Responsibility**  The customer is responsible for procedures to facilitate the implementation of the system and information integrity policy and the associated system and information integrity controls.  **Azure**  The Asset Classification Standard and Asset Protection Standard and Azure Network Security SOP implement the system and information integrity policy and associated controls and documents the following procedures:  \* Network access control  \* Routing control  \* Boundary protection  Service teams may supplement the Azure policies and procedures with offering-specific policies and procedures. Service-team-specific policies and procedures associated with access control are documented and stored within internal Azure SharePoint sites. Only personnel with authorized credentials, adequate levels of permission, legitimate need to know, and specific roles and responsibilities are given access to the service-team-specific policies or procedures. |
| **Part B**  **Customer Responsibility**  The customer is responsible for designating an official to manage the development, documentation, and dissemination of system and information integrity policy and procedures.  **Azure**  The Microsoft Information Risk Management Council (IRMC) organization is the governance body with approval responsibility for the Microsoft Security Policy (MSP) and Microsoft Security Program Policy (MSPP). The IRMC consists of representatives from security and risk management teams across Microsoft including Core Services Engineering and Operations (CSEO), Azure, and Global Security. The Customer Security and Trust: Security Engineering (CST-SE) organization manages the review and approval process and maintains the policies.  On an annual basis, the CST-SE conducts a line-by-line review of the MSP and MSPP. The Microsoft Security Policy (MSP) and Microsoft Security Program Policy (MSPP) Governance document describes each member’s role, types and frequency of review, escalation paths, approval process, and formal publishing procedures of the security policy. Throughout the year, if necessary, CST-SE may convene with the IRMC to conduct reviews after a significant review or change request. The approved policy update is published within the relevant tool on the Microsoft intranet. If service teams establish service-specific or team-specific policies, the respective service teams update the necessary policies at least annually. |
| **Part C1**  **Customer Responsibility**  The customer is responsible for reviewing and updating the current system and information integrity policy on a regular basis and following organization defined events.  **Azure**  The Azure team updates the Azure SOPs at least annually through a formal review process. If needed, the Azure team updates the SOP after a significant change affecting policy execution as well. If established, service-team-specific procedures are updated by their respective teams. The individual service teams review and update their respective SOPs at least annually and when required by a significant change. |
| **Part C2**  **Customer Responsibility**  The customer is responsible for reviewing and updating the current system and information integrity procedures on a regular basis and following organization defined events.  **Azure**  The Azure team updates the Azure SOPs at least annually through a formal review process. If needed, the Azure team updates the SOP after a significant change affecting policy execution as well. If established, service-team-specific procedures are updated by their respective teams. The individual service teams review and update their respective SOPs at least annually and when required by a significant change. |

## SI-2 Flaw Remediation

a. Identify, report, and correct system flaws;

b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;

c. Install security-relevant software and firmware updates within [within thirty (30) days of release of updates] of the release of the updates; and

d. Incorporate flaw remediation into the organizational configuration management process.

|  |
| --- |
| **SI-2 Control Summary Information** |
| Responsible Roles: Networking, Scanning |
| Parameter si-2(c): Software and firmware updates installed within 30 days of release of updates. |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SI-2 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for flaw remediation on customer-deployed resources, including the identification, reporting and correction of flaws.  **Azure**  **Flaw Identification**  To identify applicable software flaws, the C+AI Security team tracks multiple sources of information for vulnerability-related data. These sources include the Microsoft Security Response Center (MSRC), vendor websites, and other third-party websites. Updates tracked by these sources are monitored by C+AI Security for possible inclusion on its monthly security bulletins, notifications, and advisories. Based on their applicability to the Azure environment, Only a subset of these updates may be required by C+AI Security.  Microsoft publishes bulletins that include specific information relevant to the security update being released. Azure reviews vulnerabilities that are deemed to have a significant impact to the operational environment. Microsoft bulletins are disseminated to all personnel. Additional information can be found on the following websites:  \* MSRC: <https://www.microsoft.com/en-us/msrc>  \* MSRC Bulletins and Advisories: <https://msrc.microsoft.com/update-guide/>  Non-Microsoft software used in Azure to provide infrastructure services and client services is kept current for the optimal operation of the environment. Each software vendor provides information about their security updates. Vendor websites are monitored, including, but not limited to:  \* Cisco: <https://tools.cisco.com/security/center/publicationListing.x>  \* Juniper: <https://kb.juniper.net/InfoCenter/index?page=content&channel=SECURITY\_ADVISORIES>  \* TippingPoint: <https://tmc.tippingpoint.com/TMC>  \* F5 Networks: <https://www.f5.com/services/support/security-incident-response-team-sirt> and <https://support.f5.com/csp/home>  \* NetScaler: <https://support.citrix.com/securitybulletins/>  For network devices, vendors make Azure Networking aware of security vulnerabilities on their products via email. The email is logged into Azure DevOps and analysis is performed to evaluate possible risks and mitigations. Azure Networking has dedicated support engineers from the major hardware vendors, including Cisco, Juniper, and F5, that assist with the analysis and determination of the course of action. Azure Networking tracks the issue to completion. A similar process is followed with updates provided by other vendors, with the goal of matching the updates required to the current Azure environment.  The C+AI Security team monitors Azure using automated vulnerability scanning tools. These tools are configured to provide the C+AI Security team and users specific system security flaws. Azure configures these tools based on knowledge provided by vendors and other sources, including analysis by C+AI Security. The C+AI Security team conducts the following activities monthly.  On the Thursday prior to release, the C+AI Security team holds a conference call with Azure stakeholders to review updates that are required in the Azure environment, based on the data provided in the Advance Notification Service by MSRC. Minutes from this call are recorded and saved for historical understanding of the rationale used to determine which updates were required in the past.  On release day, the second Tuesday of every month, MSRC provides a review via conference call of detailed information with Azure stakeholders for inclusion on the list of updates required in the Azure environment. A consensus is reached with Azure stakeholders on the required security updates for the Azure environment. Meeting minutes record attendees and any concerns regarding all released security updates.  MSRC sends e-mail communication to broad Azure distribution lists that includes list of required updates, the download location of required software, and deadline for installation of the updates. After the email communication is sent, the same information is posted to the internal C+AI Security website for future reference.  Impact assessments are conducted for all vulnerabilities identified. The assessment encompasses multiple factors, including:  \* Access required, local or remote  \* Authentication requirements  \* Exploit availability  \* Outcome of exploitation such as remote code execution or elevation of privilege  **Flaw Correction**  The C+AI Security team assesses the vulnerability severity and criticality impact based on documented and deduced software and technology deployment and use in Azure environments. For example, Microsoft Expression Web is not used in Azure servers and therefore a vulnerability that impacts Expression Web is outside of the scope of updates required to be applied.  C+AI Security collects information from a variety of sources and scanners to help determine the inventory of applications installed in servers and the current threat surface. Specific steps in the vulnerability process include:  \* Review mitigating controls that may affect the vulnerability rating such as firewalls, Microsoft Defender for Endpoint (MDE) antivirus and anti-malware software, and ACLs  \* Review the Asset Value for the affected assets  \* Determine the timeframe for the application of the required updates  Most security updates are required to be installed within thirty (30) days of the notification of the update’s availability. C+AI Security occasionally requires an expedited timeline for the application of security updates based on the following criteria:  \* Applications or services affected  \* Availability of reliable exploit code  \* Prevalence of exploit activity  \* External regulator requirements, such as a Cybersecurity and Infrastructure Security Agency (CISA) Emergency Directive (ED)  Information collected from C+AI Security monitoring efforts or an increase on the risk level faced by Azure servers may be used to expedite remediation of outstanding security vulnerabilities after the original deadline was set. These changes are communicated to the necessary personnel.  In partnership with other Azure teams, C+AI Security collects, analyzes, and alerts the security contacts for the affected property on system and network behavior that may be deemed malicious or that could be the effect of an intrusion. In coordination with the Security Response Team, events are analyzed and, if deemed to be an incident, are handled in accordance with the Azure Incident Management Standard Operating Procedure (SOP).  Verified flaws identified for Azure as a result of the Vulnerability Scanning Tools scan process are identified and tracked as part of the Azure Plan of Actions and Milestones (POA&M) process.  **Flaw Reporting**  Reporting of security vulnerabilities is conducted via vulnerability scanning tool results. Azure provides a Vulnerability Management and Reporting Tool which provides Microsoft personnel the ability to review vulnerability data from a reporting interface. Vulnerability scans are conducted monthly at minimum. The vulnerability scan tools provide reports based on multiple criteria, including property, server, and security update. Communication from the C+AI Security team via Service 360 (S360) and email is used to notify service teams in cases of elevated risk or when expedited action is necessary. The remediation of vulnerabilities is one of the primary goals of the C+AI Security team. A variety of tools and processes are used to drive remediation:  \* Direct engagement with properties  \* Targeted efforts  \* Direct e-mail communication with service teams to drive remediation of high risk or expedited vulnerabilities.  \* Security updates deployment services |
| **Part B**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for testing updates related to flaw remediation for effectiveness and potential side effects prior to installation on customer-deployed resources.  **Azure**  Testing of software updates related to flaw remediation must follow the standard change management process as outlined in the Microsoft Change Management Standard. Service teams test possible changes to the environment to understand impacts to the security and operations of the system. Testing is also conducted via the Safe Deployment Practices (SDP). |
| **Part C**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for installing security-relevant software updates to customer-deployed resources within a customer-defined time period after the release of the update.  **Azure**  As noted in Part a, software and firmware updates required by C+AI Security for Azure are required to be installed within thirty (30) days of the notification of the update’s availability. C+AI Security requires on occasion an expedited timeline for the application of security updates based on the following criteria:  \* Applications or services affected  \* Availability of reliable exploit code  \* Prevalence of exploit activity  \* External regulator requirements, such as a Cybersecurity and Infrastructure Security Agency (CISA) Emergency Directive (ED)  Information collected from C+AI Security monitoring efforts or an increase on the risk level faced by Azure servers may be used to expedite remediation of outstanding security vulnerabilities after the original deadline was set. These changes are communicated to the necessary personnel.  Azure uses automated tools to determine whether a required security flaw has been remediated properly and the date of installation of security updates. These tools collect information from each asset and compare it to the requirements defined for each security update or vulnerability ID. |
| **Part D**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for including flaw remediation in configuration management.  **Azure**  Flaw remediation follows the standard change management process as outlined in the Microsoft Change Management Standard. The Policy Directives section describes the information required for submission of a request for change (RFC). As part of every RFC submission, an RFC must contain a detailed test outlining steps of the change, success metrics of the test, and a rollback plan as a risk mitigation procedure. The change review committee evaluates the RFC to grant approval prior to implementation in a production environment. |

### SI-2(2) - Automated Flaw Remediation Status

Determine if system components have applicable security-relevant software and firmware updates installed using [automated mechanisms to determine if applicable security-relevant software and firmware updates are installed on system components are defined;] [at least monthly].

|  |
| --- |
| **SI-2(2) Control Summary Information** |
| Responsible Roles: Scanning |
| Parameter si-02.02\_odp.01: automated scanning mechanisms |
| Parameter si-02.02\_odp.02: at least monthly |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SI-2(2) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for employing automated mechanisms to determine flaw remediation status for software and firmware updates at least monthly.  **Azure**  Azure utilizes a number of automated tools for vulnerability management. C+AI Security centrally manages these tools, and performs scanning against the Azure environment at least monthly and on-demand as needed. This scanning determines the state of information system components and assets regarding flaw remediation. Remediation of identified flaws is handled either centrally via patch deployment mechanisms or by the individual service teams. The continuous monitoring process provides centralized oversight of the remediation process and reporting to external stakeholders. |

### SI-2(3) - Time to Remediate Flaws and Benchmarks for Corrective Actions

(a) Measure the time between flaw identification and flaw remediation; and

(b) Establish the following benchmarks for taking corrective actions: [the benchmarks for taking corrective actions are defined;].

|  |
| --- |
| **SI-2(3) Control Summary Information** |
| Responsible Roles: Scanning |
| Parameter si-02.03\_odp: thirty (30) days for high risk flaws, ninety (90) days for moderate risk flaws, one hundred and eighty (180) days for low risk flaws |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SI-2(3) What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for remediating flaws within customer-deployed resources, including measuring the time between flaw identification and flaw remediation.  **Azure**  Azure scans all assets with vulnerability scanners. These scanners produce timestamps of initial flaw detections and flaw remediation and are used to calculate the time elapsed between the two. |
| **Part B**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for remediating flaws within customer-deployed resources and establishing customer-defined benchmarks for taking corrective actions.  **Azure**  To track and benchmark flaw remediation, Azure conducts reporting of security vulnerabilities via the scan results. Azure utilizes a Vulnerability Management and Reporting Tool which provides Azure personnel the ability to review vulnerability data from a reporting interface including the date the patch was made available.  Most security updates are required to be installed within thirty (30) days of the notification of the update’s availability. Verified flaws identified for Azure as a result of the monthly scan process are identified and tracked as part of the Azure Plan of Actions and Milestones (POA&M) process. |

## SI-3 Malicious Code Protection

a. Implement [Selection (OneOrMore): signature-based;non-signature-based] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code;

b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures;

c. Configure malicious code protection mechanisms to:

1. Perform periodic scans of the system [at least weekly] and real-time scans of files from external sources at [Selection (OneOrMore): endpoint;network entry and exit points] as the files are downloaded, opened, or executed in accordance with organizational policy; and

2. [Selection (OneOrMore): block malicious code;quarantine malicious code;take [administrator or defined security personnel near-realtime] ] ; and send alert to [personnel or roles to be alerted when malicious code is detected is/are defined;] in response to malicious code detection; and

d. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.

|  |
| --- |
| **SI-3 Control Summary Information** |
| Responsible Roles: Logging and Monitoring, Incident Response |
| Parameter si-03\_odp.01: signature based and non-signature based |
| Parameter si-03\_odp.02: at least weekly |
| Parameter si-03\_odp.03: endpoints and network entry and exit points |
| Parameter si-03\_odp.04: block malicious code and/or quarantine malicious code |
| Parameter si-03\_odp.05: |
| Parameter si-03\_odp.06: for Defender and ClamAV, alert Azure service team personnel and incident response personnel |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SI-3 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for protecting customer-deployed resources against malicious code by implementing either signature based; non-signature based; or both malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code.  **Azure**  **Servers**  The use of anti-malware software is a principal mechanism for protection of Azure assets from malicious software. The software, deployed and managed by Azure Security Pack (AzSecPack), detects and prevents the introduction of viruses, malware, rootkits, worms, and other malicious software onto the services. Approved tools Microsoft Defender AV and ClamAV are installed as part of the initial build on all servers, including all entry and exit points to the Azure cloud. This software provides both preventive and detective control over malicious software using signature-based protection mechanisms. In addition to signature-based detection mechanisms, Defender also utilizes behavior monitoring, network inspection, and heuristics to detect malicious code that may be missed by signature-based methods.  **Network Devices**  Network devices do not natively support anti-malware software, but are protected through a combination of the server-based anti-malware software described above and the secure coding practices required by the Security Development Lifecycle (SDL), configuration management and control, supply chain processes, and comprehensive logging and monitoring. |
| **Part B**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for automatically updating malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures.  **Azure**  **Servers**  Azure updates malicious code protection mechanisms for Defender and ClamAV including signature definitions whenever new releases are available. The anti-malware software is configured to check for updates to the signature files at least daily and automatically update the signatures accordingly.  **Network Devices**  Network devices do not natively support anti-malware software, but are protected through a combination of the server-based anti-malware software described above and the secure coding practices required by the Security Development Lifecycle (SDL), configuration management and control, supply chain processes, and comprehensive logging and monitoring. |
| **Part C1**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for protecting customer-deployed resources against malicious code by configuring mechanisms to perform periodic scans of the system at a customer-defined frequency and perform real-time scans of files from external sources at endpoint and/or network entry/exit points as the files are downloaded, opened, or executed in accordance with organizational security policy.  **Azure**  **Servers**  Defender and ClamAV are centrally managed via Azure Security Pack (AzSecPack). On each endpoint for each service team, the anti-malware software performs:  \* periodic scans at least weekly and  \* real-time scans of files as they are downloaded, opened, or executed.  **Network Devices**  Network devices do not natively support anti-malware software, but are protected through a combination of the server-based anti-malware software and the secure coding practices required by the Security Development Lifecycle (SDL), configuration management and control, supply chain processes, and in-depth logging and monitoring. |
| **Part C2**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for one or more of blocking malicious code; quarantining malicious code; or taking an organization-defined action; and sending alerts to organization-defined personnel or roles in response to malicious code detection.  **Azure**  **Servers**  When Defender detects malware, it attempts to block the malware and an alert is generated and sent to Azure service teams, Azure Security, and/or C+AI Security, depending on the severity of the malware and the outcome of Defender-initiated actions.  When ClamAV detects malware, it does not auto-remediate the malware. Instead, Microsoft Threat Intelligence Center (MSTIC) detections are used to analyze commands generated as part of process activity to look for anomalous activity. The anti-malware protection software ClamAV for Linux servers is currently not configured with on-access scanning enabled. As such, real-time scanning and protections for Linux services are not provided. To mitigate against the risk of enabling malicious files to be permitted to be copied or installed on Linux servers and remain there until found by the weekly scans, Azure has implemented strong access management controls, traffic flow restrictions, and system-level monitoring that are in place for all Azure servers including Linux.  Response to anti-malware detections are handled by a combination of the service teams for those detections that autoroute to the service owners and the Microsoft Security Response Center (MSRC) working in the Cyber Defense Operating Center (CDOC) who reviews detections for anomalous activity. The receiving personnel initiate the incident management process as applicable. For successfully blocked malware, no additional action is needed. Incidents, including false positives, are tracked and resolved, and post-mortem analysis is performed on incidents where it is determined necessary. Customers including government customers and US-CERT are notified by the incident management processes if required.  **Network Devices**  Network devices do not natively support anti-malware software, but are protected through a combination of the server-based anti-malware software and the secure coding practices required by the Security Development Lifecycle (SDL), configuration management and control, supply chain processes, and in-depth logging and monitoring. |
| **Part D**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for addressing the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.  **Azure**  **Servers**  By default, Defender quarantines malicious code identified from the anti-malware software and does not immediately delete it for the Windows operating system. Falsely identified malicious code is put in a quarantined folder on the system. Azure can roll back quarantined files if they are falsely determined to be malicious code to resolve impact to operations in the system.  For Linux operating systems, Azure uses ClamAV to identify the characteristics and behavior of malicious code. ClamAV does not auto-remediate the malware. Instead, Microsoft Threat Intelligence Center (MSTIC) detections are used to analyze commands generated as part of process activity to look for anomalous activity. Response to anti-malware detections are handled by a combination of the service teams for those detections that autoroute to the service owners and the Microsoft Security Response Center (MSRC) working in the Cyber Defense Operating Center (CDOC) who reviews detections for anomalous activity.  **Network Devices**  Network devices do not natively support anti-malware software, but are protected through a combination of the server-based anti-malware software and the secure coding practices required by the Security Development Lifecycle, configuration management and control, supply chain processes, and in-depth logging and monitoring. |

## SI-4 System Monitoring

a. Monitor the system to detect:

1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: [monitoring objectives to detect attacks and indicators of potential attacks on the system are defined;] ; and

2. Unauthorized local, network, and remote connections;

b. Identify unauthorized use of the system through the following techniques and methods: [techniques and methods used to identify unauthorized use of the system are defined;];

c. Invoke internal monitoring capabilities or deploy monitoring devices:

1. Strategically within the system to collect organization-determined essential information; and

2. At ad hoc locations within the system to track specific types of transactions of interest to the organization;

d. Analyze detected events and anomalies;

e. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation;

f. Obtain legal opinion regarding system monitoring activities; and

g. Provide [system monitoring information to be provided to personnel or roles is defined;] to [personnel or roles to whom system monitoring information is to be provided is/are defined;] [Selection (OneOrMore): as needed;[a frequency for providing system monitoring to personnel or roles is defined (if selected);] ] .

Guidance: See US-CERT Incident Response Reporting Guidelines.

|  |
| --- |
| **SI-4 Control Summary Information** |
| Responsible Roles: Logging and Monitoring, Incident Response |
| Parameter si-04\_odp.01: ensure the proper functioning of internal processes and controls in furtherance of regulatory and compliance requirements; examine system records to confirm that the system is functioning in an optimal, resilient, and secure state; identify irregularities or anomalies that are indicators of a system malfunction or compromise |
| Parameter si-04\_odp.02: Azure Security Logging and Auditing (SLAM) and C+AI Security logging and monitoring |
| Parameter si-04\_odp.03: monitoring aligned with SI-04 Part a |
| Parameter si-04\_odp.04: Service Engineer Operations |
| Parameter si-04\_odp.05: daily and as needed |
| Parameter si-04\_odp.06: |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SI-4 What is the solution and how is it implemented?** |
| **Part A1**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for monitoring customer-deployed resources to detect: attacks and indicators of potential attacks in accordance with customer-defined monitoring objectives.  **Azure**  Azure requires service teams to deploy active monitoring solutions that generate audit logs and alerts as a required step in the Security Development Lifecycle (SDL) process, described in the CM family of controls. All service teams upload their logs to Geneva Monitoring, where they are aggregated and processed as described in the AU family of controls. The Logging and Monitoring team assists in identifying normal usage of the system and deviations from that normal range. The tooling automatically reviews audit logs and antivirus and anti-malware information to confirm that the system is functioning in an optimal, resilient, and secure state and identifies irregularities or anomalies that are indicators of a system malfunction or compromise. Unusual activity is flagged for further review via detections and alerts. Any log event that indicates a potential violation of the Microsoft Security Policy (MSP) is immediately brought to the attention of Azure Security.  In addition, the implemented host-based SDN firewall uses a deny all policy. |
| **Part A2**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for monitoring customer-deployed resources to detect: unauthorized local, network, and remote connections.  **Azure**  Local connections are disallowed by policy within Azure. No personnel have local access. Azure performs network monitoring and detection of unauthorized connections via Network Isolation (NetIso), which provides the Network Risk Management Service (NRMS) for network baseline measurement, management, and enforcement. The service provides an assessment of network security and alerts on internet-exposed endpoints via Incident Management (IcM) based on analysis patterns for configuration issues. Any process that begins offering an open network port is flagged and investigated if it is not part of the approved baseline for that host to ensure detection of network services that have not been authorized as an indicator of compromise. |
| **Part B**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for monitoring customer-deployed resources to identify unauthorized use through customer-defined techniques and methods.  **Azure**  Due to the size and complexity of the Azure environment, Azure utilizes event forwarding and monitoring tools to record events across Azure and correlate the events gathered by each logging tool. Log review cannot be conducted manually in the Azure environment due to the high volume of events. Instead, Azure implements automated methods to perform review, analysis, and reporting of logs. Azure Security Monitoring (ASM) and Scuba are used to do direct alerting using IcM tickets on security-relevant events. These tools utilize event audit policies and detections that report events to the Microsoft Operations Center (MOC), Security Response Team, and service teams, as appropriate. The policies are tuned to alert on events of immediate concern. Events that need little or no correlation to prompt a preliminary investigation and attention of Security Response Team personnel.  Once processed, the Security Response Team reviews and analyzes alerts generated by the automated review of audit records in real time, specifically in the case of a security incident, customer request or escalation, or any other functionality impacting the incident in production. Groups of these correlated events that meet a pattern of a known attack methodology are collected and delivered to personnel via IcM or email. Personnel correlate alerts, collect multiple similar alarms, and append them to tickets for review and analysis. The alerting system provides response capability twenty-four (24) hours a day, seven (7) days a week. Troubleshooting Guides (TSGs) applied to workflow tickets provide instructions for the escalation of certain events to response personnel. |
| **Part C1**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for configuring monitoring devices for customer-deployed resources strategically to collect customer-defined essential information, and at ad hoc locations to track specific types of transactions of interest to the organization.  **Azure**  All assets act as monitoring devices and are configured to log all security-relevant events. Suspicious events generate alerts and notifications to service team staff and incident management staff as needed. Azure assets are configured to upload their logs to a central repository managed by C+AI Security. These logs are aggregated and reports are generated by the Security Response Team. Because of the extensive centralized management of all audit logs, Azure has determined that there is no need for ad-hoc deployment of monitoring devices. |
| **Part C2**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for configuring monitoring devices at ad hoc locations to track specific types of transactions of interest to the organization.  **Azure**  All assets act as monitoring devices and are configured to log all security-relevant events. Suspicious events generate alerts and notifications to service team staff and incident management staff as needed. Azure assets are configured to upload their logs to a central repository managed by C+AI Security. These logs are aggregated and reports are generated by the Security Response Team. Because of the extensive centralized management of all audit logs, Azure has determined that there is no need for ad-hoc deployment of monitoring devices. |
| **Part D**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for monitoring customer-deployed resources and analyze detected events and anomalies  **Azure**  Only service team personnel for the specific asset within Azure have access to security logs on the local asset via the role-based access control (RBAC) implemented via OneIdentity. Azure implements protection of audit information using an authenticated and encrypted connection from the local asset of log generation to the centralized audit collection systems using the Geneva Monitoring Agent (MA). Access to the centralized audit collection systems and storage is restricted to the Security Engineering and Operations groups based on the standard access groups defined for Azure.  Only authorized service team personnel are allowed access to the actual audit records, and their assigned rights prohibit them from modifying or deleting audit information. Even if a user is able to clear local asset log data after elevating permissions via an approved JIT request, the action of cleaning the data is logged, and the cleared log data is present on Geneva Monitoring storage due to central ingestion.  The following mechanisms are used to protect log information in transit and at rest:  \* Logs on the local asset can only be accessed through direct login to the asset.  \* The transfer of logs from the local asset to the service team and central storage accounts occurs over an HTTPS connection.  \* Read-only access to logs in Geneva Monitoring storage for Azure users is enabled through the Geneva Monitoring front-end portal. The access is restricted through AD security groups which are managed through OneIdentity. |
| **Part E**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for adjusting monitoring activity whenever there is an indication of increased risk to customer operations, assets, and individuals; other organizations; or the Nation based on law enforcement information; intelligence information, or other credible sources of information.  **Azure**  Azure Security notifies service teams if a change in the level of monitoring is necessary due to indications of increased risk, and service teams adjust monitoring accordingly. Additionally, tooling heuristics are tailored to look for specific threats based on the nature of the risk to Azure operations and assets. |
| **Part F**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for obtaining legal opinion with regard to system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.  **Azure**  Azure Security and the Security Response Team, in consultation with Corporate, External, and Legal Affairs (CELA), defines a set of log events and alerts that meet regulatory requirements for incident management and investigation. This structure is intended to support identification of known suspicious activity and to support the investigation of misuse and abuse of Azure services. To comply fully with applicable regulations, Azure service teams follow defined requirements for event collection and notification processes. |
| **Part G**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for providing selected monitoring information to customer-defined personnel/roles as needed and/or at the required frequency.  **Azure**  All services upload logs to Geneva Monitoring for aggregation and analysis. Alerts are generated from this data by Azure Security and C+AI Security. This data is available as needed. |

### SI-4(1) - System-wide Intrusion Detection System

Connect and configure individual intrusion detection tools into a system-wide intrusion detection system.

|  |
| --- |
| **SI-4(1) Control Summary Information** |
| Responsible Roles: Logging and Monitoring, Incident Response, Networking |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SI-4(1) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for monitoring customer-deployed resources, including the connection and configuration of individual intrusion detection tools into a system-wide intrusion detection system.  **Azure**  Azure assets upload logs to a central repository managed by C+AI Security. Azure Security and the Security Response Team generate consolidated reports from this data, providing system-wide intrusion detections. Additionally, a combination of detection via the logging and monitoring pipeline and alerting infrastructure and fast response address the risk of intrusion. This includes the use of event forwarding tools, security incident and event management tools, vulnerability scanning and reporting tools, and antivirus and anti-malware services. These services feed into central monitoring which alerts the Security Response Team for any events that need further investigation for central investigation or the service teams directly for alerts that are autorouted based on metadata available in Service Tree. |

### SI-4(2) - Automated Tools and Mechanisms for Real-time Analysis

Employ automated tools and mechanisms to support near real-time analysis of events.

|  |
| --- |
| **SI-4(2) Control Summary Information** |
| Responsible Roles: Logging and Monitoring, Incident Response, Networking |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SI-4(2) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for monitoring customer-deployed resources using automated tools and mechanisms to support near real-time analysis of events.  **Azure**  Due to the size and complexity of the Azure environment, Azure utilizes event forwarding and monitoring tools to record events across Azure and correlate the events gathered by each logging tool. Log review cannot be conducted manually in the Azure environment due to the high volume of events. Instead, Azure implements automated methods to perform review, analysis, and reporting of logs. Azure Security Monitoring (ASM) and Scuba are used to do direct alerting using Incident Management (IcM) tickets on security-relevant events. These tools utilize event audit policies and detections that report events to the Microsoft Operations Center (MOC) and service teams, as appropriate. The policies are tuned to alert on events of immediate concern. Events that need little or no correlation to prompt a preliminary investigation and attention of Security Response Team personnel.  Once processed, the Security Response Team reviews and analyzes alerts generated by the automated review of audit records in real time, specifically in the case of a security incident, customer request or escalation, or any other functionality impacting the incident in production. Groups of these correlated events that meet a pattern of a known attack methodology are collected and delivered to personnel via IcM or email. Personnel correlate alerts, collect multiple similar alarms, and append them to tickets for review and analysis. The alerting system provides response capability twenty-four (24) hours a day, seven (7) days a week. Troubleshooting Guides (TSGs) applied to workflow tickets provide instructions for the escalation of certain events to response personnel. |

### SI-4(4) - Inbound and Outbound Communications Traffic

(a) Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic;

(b) Monitor inbound and outbound communications traffic [continuously] for [Assignment: organization-defined unusual or unauthorized activities or conditions].

|  |
| --- |
| **SI-4(4) Control Summary Information** |
| Responsible Roles: Logging and Monitoring, Incident Response, Networking |
| Parameter si-4.4\_prm\_1: continuously |
| Parameter si-4.4\_prm\_2: unusual or unauthorized activities or conditions |
| Parameter si-04.04\_odp.01: |
| Parameter si-04.04\_odp.02: |
| Parameter si-04.04\_odp.03: |
| Parameter si-04.04\_odp.04: |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SI-4(4) What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for determining criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic.  **Azure**  Azure currently has detections in place that will alert on suspicious/malicious inbound and outbound network activities to include brute force attacks, distributed denial of service, communication with known malicious IPs, and cryptocurrency mining.  Azure filters network traffic to Azure subscriptions at the Management Group Level. All traffic not allowed by the relevant Network Baselines will be blocked, regardless of Network Security Group (NSG) configuration within Azure Subscriptions. Traffic is effectively filtered at each level of the resource stack. In order for network traffic to get to an asset, it needs to be allowed by all of the levels of security rules. |
| **Part B**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for monitoring customer-deployed resources, including the monitoring of inbound and outbound communications traffic at the customer-defined frequency for unusual or unauthorized activities/conditions.  **Azure**  Azure monitors communications continually using the centralized monitoring, correlation, and analysis systems that manage the large amount of information generated by assets within the environment. In addition to standard logging and monitoring via asset logs described in the AU family, Azure performs network monitoring and detection of unauthorized connections via Network Isolation (NetIso), which provides the Network Risk Management Service (NRMS) for network baseline measurement, management, and enforcement. The service provides an assessment of network security and alerts on internet-exposed endpoints via Incident Management (IcM) based on analysis patterns for configuration issues. Any process that begins offering an open network port is flagged and investigated if it is not part of the approved baseline for that host to ensure detection of network services that have not been authorized as an indicator of compromise.  Azure filters network traffic to Azure subscriptions at the Management Group Level. All traffic not allowed by the relevant Network Baselines will be blocked, regardless of Network Security Group (NSG) configuration within Azure Subscriptions. Traffic is effectively filtered at each level of the resource stack. In order for network traffic to get to an asset, it needs to be allowed by all of the levels of security rules. |

### SI-4(5) - System-generated Alerts

Alert [personnel or roles to be alerted when indications of compromise or potential compromise occur is/are defined;] when the following system-generated indications of compromise or potential compromise occur: [compromise indicators are defined;].

Guidance: In accordance with the incident response plan.

|  |
| --- |
| **SI-4(5) Control Summary Information** |
| Responsible Roles: Logging and Monitoring, Incident Response, Networking |
| Parameter si-04.05\_odp.01: roles defined in the Azure Incident Management Standard Operating Procedure (SOP) |
| Parameter si-04.05\_odp.02: criteria defined in the Azure Incident Management Standard Operating Procedure (SOP) |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SI-4(5) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for providing monitoring alerts for customer-deployed resources to customer-defined personnel or roles when specified indications of compromise or potential compromise occur.  **Azure**  Due to the size and complexity of the Azure environment, Azure utilizes event forwarding and monitoring tools to record events across Azure and correlate the events gathered by each logging tool. Log review cannot be conducted manually in the Azure environment due to the high volume of events. Instead, Azure implements automated methods to perform review, analysis, and reporting of logs. Azure Security Monitoring (ASM) and Scuba are used to do direct alerting using Incident Management (IcM) tickets on security-relevant events. These tools utilize event audit policies and detections that report events to the Security Response Team and service teams as appropriate.  Once processed, the Security Response Team reviews and analyzes alerts generated by the automated review of audit records in real time. Events that meet a pattern of a known attack methodology are delivered to the appropriate service teams via IcM or email. These teams review and analyze the activities detailed in the alerts in accordance with Troubleshooting Guides (TSGs) attached to the ticketed alert. The alerting system provides 24/7 response capability. |

### SI-4(10) - Visibility of Encrypted Communications

Make provisions so that [encrypted communications traffic to be made visible to system monitoring tools and mechanisms is defined;] is visible to [system monitoring tools and mechanisms to be provided access to encrypted communications traffic are defined;].

Requirement: The service provider must support Agency requirements to comply with M-21-31 (https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-31-Improving-the-Federal-Governments-Investigative-and-Remediation-Capabilities-Related-to-Cybersecurity-Incidents.pdf) and M-22-09 (https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf).

|  |
| --- |
| **SI-4(10) Control Summary Information** |
| Responsible Roles: Logging and Monitoring, Networking |
| Parameter si-04.10\_odp.01: organization-defined encrypted communications traffic |
| Parameter si-04.10\_odp.02: organization-defined information system monitoring tools and mechanisms |
| Implementation Status (check all that apply):  ☐ Implemented  ☒ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SI-4(10) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for making provisions so that customer-defined encrypted communications traffic is visible to information system monitoring tools.  **Azure**  For Azure services, onboarding to Azure Security Pack (AzSecPack) enables monitoring of network communication correlated with network logs and in-memory lateral movement during post exploitation for all deployment types via Process Investigation, which is available externally via Microsoft Defender for Cloud via Fileless Attack detections, and via the Network Risk Management (NRM) Service. The NRM service assesses the resultant set of open ports and protocols based on data provided by the VM agent. Additionally, for VMs hosted on Azure, the Network Security Group (NSG) settings are considered and the resultant set of the settings is calculated. Additionally, for the assets running in Bare Metal, Azure assesses the Surface Area Manager configuration settings. For Linux VMs hosted in Azure, Azure uses the NSG settings to validate that the configuration meets the network baseline requirements. For all deployment types, if there is a network baseline violation that exposes a management port to the internet, an alert is generated and routed to the service team.  For internal service teams, Azure implements monitoring and alerting for unusual behavior of key security features including, but not limited to, if a user accesses an asset without using Azure Just In Time (JIT) access, if a dSTS account has an unusual access pattern, if the Geneva Actions have unusual activity, if the Azure Fabric is accessed without using Azure JIT, or if a service owner has unexpected changes to permissions in the service team subscription.  Additionally, internal services regardless of deployment type monitor their own network connections for unexpected network activities at the application layer. However, to protect customer end user identifiable information, Azure does not monitor the customer traffic in the security monitoring solutions. |

### SI-4(11) - Analyze Communications Traffic Anomalies

Analyze outbound communications traffic at the external interfaces to the system and selected [interior points within the system where communications traffic is to be analyzed are defined;] to discover anomalies.

|  |
| --- |
| **SI-4(11) Control Summary Information** |
| Responsible Roles: Logging and Monitoring |
| Parameter si-04.11\_odp: key interior points within Azure |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SI-4(11) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for analyzing communications traffic anomalies for customer-deployed resources, including an analysis of outbound communications traffic at the external boundary and at customer-defined interior points within the system to discover anomalies.  **Azure**  For Azure services, onboarding to Azure Security Pack (AzSecPack) enables monitoring of network communication correlated with network logs and in-memory lateral movement during post exploitation for all deployment types via Process Investigation, which is available externally via Microsoft Defender for Cloud via Fileless Attack detections, and via the Network Risk Management (NRM) Service. The NRM service assesses the resultant set of open ports and protocols based on data provided by the VM agent. Additionally, for VMs hosted on Azure, the Network Security Group (NSG) settings are considered and the resultant set of the settings is calculated. Additionally, for the assets running in Bare Metal, Azure assesses the Surface Area Manager configuration settings. For Linux VMs hosted in Azure, Azure uses the NSG settings to validate that the configuration meets the network baseline requirements. For all deployment types, if there is a network baseline violation that exposes a management port to the internet, an alert is generated and routed to the service team.  For internal service teams, Azure implements monitoring and alerting for unusual behavior of key security features including, but not limited to, if a user accesses an asset without using Azure Just In Time (JIT) access, if a dSTS account has an unusual access pattern, if the Geneva Actions have unusual activity, if the Azure Fabric is accessed without using Azure JIT, or if a service owner has unexpected changes to permissions in the service team subscription.  Additionally, internal services regardless of deployment type monitor their own network connections for unexpected network activities at the application layer. However, to protect customer end user identifiable information, Azure does not monitor the customer traffic in the security monitoring solutions. |

### SI-4(12) - Automated Organization-generated Alerts

Alert [personnel or roles to be alerted when indications of inappropriate or unusual activity with security or privacy implications occur is/are defined;] using [automated mechanisms used to alert personnel or roles are defined;] when the following indications of inappropriate or unusual activities with security or privacy implications occur: [activities that trigger alerts to personnel or are defined;].

|  |
| --- |
| **SI-4(12) Control Summary Information** |
| Responsible Roles: Incident Response |
| Parameter si-04.12\_odp.01: Microsoft Operations Center (MOC) and service teams |
| Parameter si-04.12\_odp.02: Azure Security Monitoring (ASM), Scuba, and/or Incident Management (IcM) |
| Parameter si-04.12\_odp.03: when there are threats identified by authoritative sources (e.g. CTOs) and IAW with CJCSM 6510.01B |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SI-4(12) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for alerting security personnel using automated mechanisms of customer-defined inappropriate or unusual activities with security and privacy implications occur.  **Azure**  When Azure Security receives notification of inappropriate or unusual activities, they alert appropriate personnel using automated mechanisms such as Azure DevOps, Incident Management (IcM), Service 360 (S360), and email. |

### SI-4(14) - Wireless Intrusion Detection

Employ a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises or breaches to the system.

|  |
| --- |
| **SI-4(14) Control Summary Information** |
| Responsible Roles: Datacenter Hosting |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SI-4(14) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for employing a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises or breaches to customer managed resources.  **Azure**  Wireless access is not permitted within the Azure environment. Azure regularly scans for rogue wireless signals at least quarterly within the Azure datacenters. Results are logged and documented by the Azure Security Response Team. Any rogue signals are investigated and removed. The involvement of the Azure Security Response Team will initiate the processes outlined on the IR control family section of this SSP. Refer to that IR control family section to identify incident response processes and procedures. |

### SI-4(16) - Correlate Monitoring Information

Correlate information from monitoring tools and mechanisms employed throughout the system.

|  |
| --- |
| **SI-4(16) Control Summary Information** |
| Responsible Roles: Logging and Monitoring |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SI-4(16) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for correlating information from monitoring tools and mechanisms employed throughout the system.  **Azure**  All Azure assets upload logs to Geneva Monitoring for aggregation and analysis. Reports are generated from this data and cover system-wide intrusion detections. |

### SI-4(18) - Analyze Traffic and Covert Exfiltration

Analyze outbound communications traffic at external interfaces to the system and at the following interior points to detect covert exfiltration of information: [interior points within the system where communications traffic is to be analyzed are defined;].

|  |
| --- |
| **SI-4(18) Control Summary Information** |
| Responsible Roles: Logging and Monitoring |
| Parameter si-04.18\_odp: key interior points within Azure |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SI-4(18) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for analyzing communications traffic for customer-deployed resources, including an analysis of outbound communications traffic at the external boundary and at customer-defined interior points within the system to detect covert exfiltration of information.  **Azure**  For Azure services, onboarding to Azure Security Pack (AzSecPack) enables monitoring of network communication correlated with network logs and in-memory lateral movement during post exploitation for all deployment types via Process Investigation, which is available externally via Microsoft Defender for Cloud via Fileless Attack detections, and via the Network Risk Management (NRM) Service. The NRM service assesses the resultant set of open ports and protocols based on data provided by the VM agent. Additionally, for VMs hosted on Azure, the Network Security Group (NSG) settings are considered and the resultant set of the settings is calculated. Additionally, for the assets running in Bare Metal, Azure assesses the Surface Area Manager configuration settings. For Linux VMs hosted in Azure, Azure uses the NSG settings to validate that the configuration meets the network baseline requirements. For all deployment types, if there is a network baseline violation that exposes a management port to the internet, an alert is generated and routed to the service team.  For internal service teams, Azure implements monitoring and alerting for unusual behavior of key security features including, but not limited to, if a user accesses an asset without using Azure Just In Time (JIT) access, if a dSTS account has an unusual access pattern, if the Geneva Actions have unusual activity, if the Azure Fabric is accessed without using Azure JIT, or if a service owner has unexpected changes to permissions in the service team subscription.  Additionally, internal services regardless of deployment type monitor their own network connections for unexpected network activities at the application layer. However, to protect customer end user identifiable information, Azure does not monitor the customer traffic in the security monitoring solutions. |

### SI-4(19) - Risk for Individuals

Implement [additional monitoring of individuals who have been identified as posing an increased level of risk is defined;] of individuals who have been identified by [sources that identify individuals who pose an increased level of risk are defined;] as posing an increased level of risk.

|  |
| --- |
| **SI-4(19) Control Summary Information** |
| Responsible Roles: Incident Response |
| Parameter si-04.19\_odp.01: additional monitoring as defined by Azure service teams |
| Parameter si-04.19\_odp.02: HR and engineering groups |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SI-4(19) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for monitoring individuals who pose a greater risk.  **Azure**  In the case where Azure identifies an individual as posing an increased level of risk, that individual’s access is revoked. The Security Response Team takes special interest in data generated by existing monitoring solutions to identify any malicious actions the individual may attempt. The Security Response Team responds to requests by HR and engineering groups to take emergency actions on high risk accounts, such as rapid account disablement. The Security Response Team also maintains auditable events of account activity that can be used in Security Response Team investigations. |

### SI-4(20) - Privileged Users

Implement the following additional monitoring of privileged users: [additional monitoring of privileged users is defined;].

|  |
| --- |
| **SI-4(20) Control Summary Information** |
| Responsible Roles: Logging and Monitoring, Incident Response |
| Parameter si-04.20\_odp: additional monitoring as defined by Azure service teams |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SI-4(20) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for monitoring privileged users.  **Azure**  The Security Response Team uses all logs and tools to monitor personnel as necessary. In addition to the auditable event activity, custom alerts are generated for specific elevated access user accounts such as local administrators. The alerts are investigated by the Security Response Team in accordance with the incident management procedures. |

### SI-4(22) - Unauthorized Network Services

(a) Detect network services that have not been authorized or approved by [authorization or approval processes for network services are defined;] ; and

(b) [Selection (OneOrMore): audit;alert [personnel or roles to be alerted upon the detection of network services that have not been authorized or approved by authorization or approval processes is/are defined (if selected);] ] when detected.

|  |
| --- |
| **SI-4(22) Control Summary Information** |
| Responsible Roles: Logging and Monitoring |
| Parameter si-04.22\_odp.01: Azure Change and Release Management process |
| Parameter si-04.22\_odp.02: alert the Azure LiveSite team |
| Parameter si-04.22\_odp.03: |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SI-4(22) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for detecting network services that have not been authorized or approved by customer-defined processes, and for auditing or alerting customer-defined personnel or roles.  **Azure**  Azure detects network services that have not been authorized or approved by the Azure Change and Release Management process. If an unauthorized network service is discovered, the Azure LiveSite (WALS) team investigates the issue following the incident management process. Azure tracks network connections that are opened by the processes running on the host. Any process that begins offering an open network port is flagged and investigated if it is not part of the approved baseline for that host, ensure detection of network services that have not been authorized as an indicator of compromise. In addition, the implemented host-based SDN firewall uses a default deny all policy.  Azure enforces a default deny policy which restricts communication to certain areas by firewall zones that are explicitly permitted. For any policy change, a detailed request with justification must be submitted and approved by C+AI Security through the standard security process. |

### SI-4(23) - Host-based Devices

Implement the following host-based monitoring mechanisms at [system components where host-based monitoring is to be implemented are defined;]: [host-based monitoring mechanisms to be implemented on system components are defined;].

|  |
| --- |
| **SI-4(23) Control Summary Information** |
| Responsible Roles: Logging and Monitoring |
| Parameter si-04.23\_odp.01: all hosts |
| Parameter si-04.23\_odp.02: audit logging in accordance with the AU family |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SI-4(23) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for implementing host-based monitoring for customer-deployed resources.  **Azure**  All hosts within Azure have event logging enabled. If this functionality is turned off or unsuccessful, an alert is generated through Geneva Monitoring and the alert is investigated as a security incident. Assets are each configured with an Event Forwarding Tool. The Event Forwarding Tool sends audit records to the Security Incident and Event Management Tool via an event collection infrastructure which also archives security events within the environment. This event forwarding occurs in real time for the interconnected system. Additionally, antivirus and anti-malware software is configured to scan, real-time, files incoming to the system and quarantines them if determined to be malicious. Alerts from clients are logged in the antivirus and anti-malware software database and the alerts for malware-related events are sent in near-real time to the Security Response Team three ways. This happens via alerts/tickets, emails to Security Response Team, and a feed to the security incident and event management tool.  Azure Security Pack (AzSecPack) enables monitoring of network communication correlated with network logs and in-memory lateral movement during post exploitation for all deployment types via Process Investigation, which is available externally via Fileless Attack detections from Microsoft Defender for Cloud, and via the Network Risk Management (NRM) Service. AzSecPack is automatically enabled for applicable Azure assets via a centrally managed configuration. Monitoring of missing AzSecPack is implemented by Azure Security Monitoring (ASM). |

## SI-5 Security Alerts, Advisories, and Directives

a. Receive system security alerts, advisories, and directives from [to include US-CERT and Cybersecurity and Infrastructure Security Agency (CISA) Directives] on an ongoing basis;

b. Generate internal security alerts, advisories, and directives as deemed necessary;

c. Disseminate security alerts, advisories, and directives to: [Selection (OneOrMore): [personnel or roles to whom security alerts, advisories, and directives are to be disseminated is/are defined (if selected);] ;[elements within the organization to whom security alerts, advisories, and directives are to be disseminated are defined (if selected);] ;[external organizations to whom security alerts, advisories, and directives are to be disseminated are defined (if selected);] ] ; and

d. Implement security directives in accordance with established time frames, or notify the issuing organization of the degree of noncompliance.

Requirement: Service Providers must address the CISA Emergency and Binding Operational Directives applicable to their cloud service offering per FedRAMP guidance. This includes listing the applicable directives and stating compliance status.

|  |
| --- |
| **SI-5 Control Summary Information** |
| Responsible Roles: Scanning |
| Parameter si-05\_odp.01: customer and regulator CERTs, US-CERT, and Cybersecurity and Infrastructure Security Agency (CISA) |
| Parameter si-05\_odp.02: C+AI Security, C+AI Security Incident Response (SIR), Azure Security and Compliance, Azure Livesite, Patch Triage Team, RDOS Team, SQL DB teams |
| Parameter si-05\_odp.03: |
| Parameter si-05\_odp.04: |
| Parameter si-05\_odp.05: |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SI-5 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for receiving security alerts, advisories, and directives from customer-defined external organizations on an ongoing basis.  **Azure**  For all asset types, Azure receives information system security alerts, advisories, and directives from external vendors, parties providing software within the Azure environment, and external security organizations including customer and regulator CERTs and other external parties performing independent vulnerability analysis. In addition, customers can report security incidents at any time through the Azure Management Portal or via a twenty-four (24) hours a day, seven (7) days a week dedicated phone line that is available.  Internally, Microsoft’s Security Response Team notifies service teams of security incidents and the latest security patches for Microsoft’s software platforms. The Microsoft Security Response Center (MSRC) also publishes Security Bulletins and associated patches every month except when MSRC determines that an out-of-band patch is required for addressing zero-day vulnerabilities or escalations. Working with MSRC and Security Response Team, external parties such as regulators, law enforcement, ISPs, and other partners can identify security issues. Service teams also subscribe to service-specific alerts, advisories, and directives as needed.  Azure is also made aware of any directives or advisories through many sources, including the FedRAMP Program Management Office (PMO), the Department of Defense (DoD) authorizing officials, and other authorizing officials, which send email alerts to provide situational awareness and any actions that all CSPs or government agencies must take. |
| **Part B**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for generating internal security alerts, advisories, and directives as deemed necessary.  **Azure**  Internally, Microsoft’s Security Response Team notifies service teams of security incidents which occur within the physical environment against Azure datacenters and boundary network devices. MSRC notifies service teams around the latest security patches for Microsoft’s software platforms. MSRC also publishes Security Bulletins and associated patches on the second Tuesday of every month except when MSRC determines that an out-of-band patch is required for addressing zero-day vulnerabilities or escalations. |
| **Part C**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for disseminating security alerts, advisories, and directives to: customer-defined personnel/roles, organizational elements, and/or external organizations.  **Azure**  Azure disseminates alerts received from vendors and other third-party services such as IBM Internet Security Systems and customer and regulator CERTs and shares this information throughout the organization. Additionally, Microsoft publishes bulletins through the Microsoft Security Response Center (MSRC) which include specific information relevant to security updates being released. The Azure Security team also addresses notifications and disseminates security alerts via email and RSS feeds received directly from external organizations other than the Services Operation Center or Microsoft Support.  **Servers**  The Vulnerability Management team conducts a monthly conference call with Azure stakeholders to review updates that are required in the environment, based on the data provided in the Advance Notification Service by the MSRC. Minutes from this call are recorded and saved for historical understanding of the rationale used to determine which updates were required in the past.  **Network Devices**  For network devices, hardware vendors make Azure Networking aware of security vulnerabilities on their products via e-mail. Azure Networking logs the email into the ticketing system and performs analysis to evaluate possible risks and mitigations. Azure Networking has dedicated support engineers from the major hardware vendors, including, but not limited to, Cisco, Juniper, and F5, that assist with the analysis and determination of the course of action. The issue is tracked by Azure Networking to completion. |
| **Part D**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for implementing security directives in accordance with established time frames or notifying the issuing organization of the degree of noncompliance.  **Azure**  Azure conducts an analysis on the list of security directives provided by the C+AI Security team to confirm applicability to Azure assets. On completion of the analysis, the Azure service teams prepare the Final Monthly Patch List specifying the vulnerabilities that must be patched. Security remediation are implemented as follows:  \* Remediation for High risk vulnerabilities are implemented within thirty (30) days of the vulnerability mitigation being released by the vendor.  \* Remediation for Medium Risk vulnerabilities are implemented within ninety (90) days of vulnerability the vulnerability mitigation being released by the vendor.  \* Low Risk vulnerabilities are risk-reviewed by Azure Security. Many Low Risk scan results are determined by Azure Security to pose no risk to Azure. In this case an exception is filed, and the result is not remediated. If the result is determined to pose any risk to Azure, remediation is implemented within one hundred and eighty (180) days.  Azure Security verifies degree of compliance using vulnerability scanners deployed in Azure.  **Servers**  On receipt of the list of updates from MSRC, the RDOS and IPAK teams conduct an analysis to determine the applicability of the patches for managed OS with the intent that all patches excepting those that are specifically not applicable to the code running on their servers are applied. If the RDOS and IPAK teams decide not to apply a patch as it is not applicable for the base images used in the environment, then the RDOS and IPAK teams create a patch exception request ticket in DevOps. This request is then reviewed and approved by the Azure Security team. A justification for not selecting the patches including the details of the non-applicable patches is documented in DevOps. The patch is deemed applicable even if a process that could exploit the vulnerability is not running but is installed in the environment.  **Network Devices**  For network devices, hardware vendors make Azure Networking aware of security vulnerabilities on their products via e-mail. Azure Networking logs the email into the ticketing system and performs analysis to evaluate possible risks and mitigations. Azure Networking has dedicated support engineers from the major hardware vendors, including, but not limited to, Cisco, Juniper, and F5, that assist with the analysis and determination of the course of action. The issue is tracked by Azure Networking to completion. |

### SI-5(1) - Automated Alerts and Advisories

Broadcast security alert and advisory information throughout the organization using [automated mechanisms used to broadcast security alert and advisory information throughout the organization are defined;].

|  |
| --- |
| **SI-5(1) Control Summary Information** |
| Responsible Roles: Scanning |
| Parameter si-05.01\_odp: Microsoft web site updates, Kusto, Jarvis, Service 360 (S360), and Incident Management (IcM) |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SI-5(1) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for using automated mechanisms to make security alert and advisory information available throughout the organization.  **Azure**  Microsoft publishes bulletins that include specific information relevant to security updates being released. Microsoft security bulletins are available to all personnel and can be found at the link below.  <https://www.microsoft.com/en-us/msrc/technical-security-notifications>  Personnel can subscribe to this notification service. In addition, Microsoft utilizes automated tools and mechanisms such as Kusto, Jarvis, Service 360 (S360), and Incident Management (IcM) to follow up on alert-related communications for service teams. |

## SI-6 Security and Privacy Function Verification

a. Verify the correct operation of [Assignment: organization-defined security and privacy functions];

b. Perform the verification of the functions specified in SI-6a [Selection (OneOrMore): [to include upon system startup and/or restart] ;upon command by user with appropriate privilege;[at least monthly] ] ;

c. Alert [to include system administrators and security personnel] to failed security and privacy verification tests; and

d. [Selection (OneOrMore): shut the system down;restart the system;[alternative action(s) to be performed when anomalies are discovered are defined (if selected);] ] when anomalies are discovered.

|  |
| --- |
| **SI-6 Control Summary Information** |
| Responsible Roles: Logging and Monitoring, Networking |
| Parameter si-6(a): Azure security and privacy functions |
| Parameter si-06\_odp.01: |
| Parameter si-06\_odp.02: |
| Parameter si-06\_odp.03: upon start up, restart, and continuously as described below |
| Parameter si-06\_odp.04: |
| Parameter si-06\_odp.05: |
| Parameter si-06\_odp.06: service engineer personnel |
| Parameter si-06\_odp.07: initiates the Incident Response process and notifies system administrators and security personnel |
| Parameter si-06\_odp.08: |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SI-6 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for security and privacy function verification for customer-deployed resources.  **Azure**  **Servers**  Azure performs near-real-time auditing and periodic verification of the following security functions to confirm their operating effectiveness. Azure uses applications called Geneva Monitoring Runners to monitor the collected data and report on the overall health of the system. If the overall health of system is deemed inappropriate for the environment by the system, the Fabric Controller (FC) is notified, and the unhealthy system is shut down and a new healthy system is brought up and running. If Azure DevOps or Incident Management (IcM) tickets are created for any security events including but not limited to alerts, advisories, and anomalies, and health status, the Windows Azure LiveSite (WALS) team actively works issues until resolution. The WALS team is staffed twenty-four (24) hours a day, seven (7) days a week.  Azure uses the logging and monitoring pipeline and event audit policies to capture security functions and perform alerting in near-real time. Azure sends automated alerts to the Security Response Team in the event of anomalies being discovered for triage, investigation, and remediation, and also alerts upon system startup and/or restart and continuously provides event monitoring and alerting to the Security Response Team.  **Network Devices**  Azure uses Config Policy Verifier (CPV) and Config Change Reporter (CCR) to verify correct operation of security functions of network devices on a continuous basis. CPV and CCR automatically send alerts to the network device monitoring tool alarm console regarding deviations of correct operations of security functions. The tools alert upon system startup and/or restart and continuously provide event monitoring and alerting to the Microsoft Operations Center (MOC). The consoles reside with the MOC, which provides analysis and routing to the Azure Networking team for remediation. CPV and CCR backs up the configuration of network devices, allowing the Azure Networking team to know who made what changes to the system. This captures all changes to the device configuration including any related to security functions and deviations from baselines. |
| **Part B**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for security and privacy function verification for customer-deployed resources at customer-defined system transitional states (e.g., startup, restart, shutdown, abort), upon command by a user with appropriate privilege, and/or at a customer-defined frequency.  **Azure**  The audit logging and monitoring pipeline alerts upon system startup and/or restart and continuously provide event monitoring and alerting to the Security Response Team and Microsoft Operations Center (MOC). |
| **Part C**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for security function verification for customer-deployed resources and notifying customer-defined personnel/roles of failed security and privacy verification tests.  **Azure**  The audit logging and monitoring pipeline alerts upon system startup and/or restart and continuously provide event monitoring and alerting to the Security Response Team and Microsoft Operations Center (MOC). |
| **Part D**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for security function verification for customer-deployed resources and whether shutdown, restart, and/or an alternative customer-defined action is taken when anomalies are discovered.  **Azure**  The monitoring tools identified above generate alerts to service team personnel in the case of security functionality failure. Depending on the type of issue, Azure DevOps or IcM tickets are opened to track resolution of the alert following the incident management process. |

## SI-7 Software, Firmware, and Information Integrity

a. Employ integrity verification tools to detect unauthorized changes to the following software, firmware, and information: [Assignment: organization-defined software, firmware, and information] ; and

b. Take the following actions when unauthorized changes to the software, firmware, and information are detected: [Assignment: organization-defined actions].

|  |
| --- |
| **SI-7 Control Summary Information** |
| Responsible Roles: Logging and Monitoring, Networking, SDL, Scanning |
| Parameter si-7(a): software, firmware, and information |
| Parameter si-7(b): automated corrective actions or alerts |
| Parameter si-07\_odp.01: |
| Parameter si-07\_odp.02: |
| Parameter si-07\_odp.03: |
| Parameter si-07\_odp.04: |
| Parameter si-07\_odp.05: |
| Parameter si-07\_odp.06: |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SI-7 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for protecting software and information integrity for customer-deployed resources.  **Azure**  **Servers**  Azure software updates are thoroughly reviewed for any unauthorized changes before entering the production environments as part of the Security Development Lifecycle (SDL) and Change and Release Management processes. Any code changes are reviewed and approved before they are deployed to the Azure production environment. Additionally, builds are digitally signed before they are deployed. If this integrity verification fails at deployment, the deployment operation fails, and the process needs to be started over.  Azure components have a set of runners which leverage information captured by Geneva Monitoring to run automated tests for checking the health of the components. Runners automatically generate alerts if any component health discrepancies are identified. This ensures recently deployed software should be propagated to more assets or rolled back as health indicators dictate.  Azure also utilizes Qualys and Azure Security Monitoring (ASM) for integrity scanning to reduce the risk of software components and devices potentially being tampered within the Azure environment. ASM has components that observe, analyze, and report on security events in Azure environment. It complements the Azure security model by examining constraints that should always remain valid, which includes configuration settings.  The Windows operating systems provide real-time file integrity validation, protection, and recovery of core system files that are installed as part of Windows or authorized Windows system updates. Windows Resource Protection (WRP) automatically detects and restores the original version of protected files if a program uses an unauthorized method to change those files. WRP provides protection for system files using two mechanisms. The first mechanism runs in the background. This protection is triggered after WRP receives a directory change notification for a file in a protected directory. After WRP receives this notification, WRP determines which file was changed. If the file is protected, WRP looks up the file signature in a catalog file to determine if the new file is the correct version. If the file is not the correct version, WRP replaces the new file with the file from the system protected cache folder (if it is in the cache folder) or from the installation source.  In addition to WRP, on demand validation and recovery of core Windows system files are provided using the System File Checker (sfc.exe) tool.  File Integrity Monitoring (FIM) consists of two elements: system file protection provided by WRP for server baselines, which is built into the operating system; and critical file monitoring provided by a combination of Local Security Policy settings for Windows Audit Object Access together with the appropriate system access control list applied to the files designated as application-critical. WRP is a real-time solution that performs scanning on a continuous basis.  Azure detects changes made to the environment through the Service Fabric and configuration platform, and custom service Monitoring Agents. Changes are detected in real time and the service provisioning and configuration platform performs predefined steps to compare integrity of operating software against released production software versions and reimage the Guest OS with appropriate software files or shut down/restart the Guest OS. If the issue is not resolved by these means, then the system is reimaged, or an alert is generated to the service team.  **Network Devices**  Azure uses Config Policy Verifier (CPV) and Config Change Reporter (CCR) to notify the Azure Networking team on unauthorized changes to network devices on a continuous basis. CPV and CCR automatically send alerts to the network device monitoring tool alarm console regarding deviations of correct operations of security functions. CPV and CCR send alerts upon system startup and/or restart and continuously provide event monitoring and alerting to the Microsoft Operations Center (MOC). The network device monitoring tool consoles reside with the MOC, which provides analysis and routing to the Azure Networking team for remediation. CPV and CCR back up the configuration of network devices, allowing the Azure Networking team to know who made what changes to the system. This captures all changes to the device configuration including who made what changes when. CPV and CCR are real-time solutions that performs scanning on a continuous basis.  **Azure Services**  In addition to the Azure standard tooling and processes, service teams may use SCOM to monitor Windows operating systems. SCOM provides file integrity validation and protection, as well as the recovery of core system files if any unauthorized changes are detected. |
| **Part B**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for taking action when unauthorized changes to the customer-deployed resources are detected.  **Azure**  **Servers**  Azure software updates are thoroughly reviewed for any unauthorized changes before entering the production environments as part of the Security Development Lifecycle (SDL) and Change and Release Management processes. Any code changes are reviewed and approved before they are deployed to the Azure production environment. Additionally, builds are digitally signed before they are deployed. If this integrity verification fails at deployment, the deployment operation fails, and the process needs to be started over.  Azure components have a set of runners which leverage information captured by Geneva Monitoring to run automated tests for checking the health of the components. Runners automatically generate alerts if any component health discrepancies are identified. This ensures recently deployed software should be propagated to more assets or rolled back as health indicators dictate.  Azure also utilizes Qualys and Azure Security Monitoring (ASM) for integrity scanning to reduce the risk of software components and devices potentially being tampered within the Azure environment. ASM has components that observe, analyze, and report on security events in Azure environment. It complements the Azure security model by examining constraints that should always remain valid, which includes configuration settings.  The Windows operating systems provide real-time file integrity validation, protection, and recovery of core system files that are installed as part of Windows or authorized Windows system updates. Windows Resource Protection (WRP) automatically detects and restores the original version of protected files if a program uses an unauthorized method to change those files. WRP provides protection for system files using two mechanisms. The first mechanism runs in the background. This protection is triggered after WRP receives a directory change notification for a file in a protected directory. After WRP receives this notification, WRP determines which file was changed. If the file is protected, WRP looks up the file signature in a catalog file to determine if the new file is the correct version. If the file is not the correct version, WRP replaces the new file with the file from the system protected cache folder (if it is in the cache folder) or from the installation source.  In addition to WRP, on demand validation and recovery of core Windows system files are provided using the System File Checker (sfc.exe) tool.  File Integrity Monitoring (FIM) consists of two elements: system file protection provided by WRP for server baselines, which is built into the operating system; and critical file monitoring provided by a combination of Local Security Policy settings for Windows Audit Object Access together with the appropriate system access control list applied to the files designated as application-critical. WRP is a real-time solution that performs scanning on a continuous basis.  Azure detects changes made to the environment through the Service Fabric and configuration platform, and custom service Monitoring Agents. Changes are detected in real time and the service provisioning and configuration platform performs predefined steps to compare integrity of operating software against released production software versions and reimage the Guest OS with appropriate software files or shut down/restart the Guest OS. If the issue is not resolved by these means, then the system is reimaged, or an alert is generated to the service team.  **Network Devices**  Azure uses Config Policy Verifier (CPV) and Config Change Reporter (CCR) to notify the Azure Networking team on unauthorized changes to network devices on a continuous basis. CPV and CCR automatically send alerts to the network device monitoring tool alarm console regarding deviations of correct operations of security functions. CPV and CCR send alerts upon system startup and/or restart and continuously provide event monitoring and alerting to the Microsoft Operations Center (MOC). The network device monitoring tool consoles reside with the MOC, which provides analysis and routing to the Azure Networking team for remediation. CPV and CCR back up the configuration of network devices, allowing the Azure Networking team to know who made what changes to the system. This captures all changes to the device configuration including who made what changes when. CPV and CCR are real-time solutions that performs scanning on a continuous basis.  **Azure Services**  In addition to the Azure standard tooling and processes, service teams may use SCOM to monitor Windows operating systems. SCOM provides file integrity validation and protection, as well as the recovery of core system files if any unauthorized changes are detected. |

### SI-7(1) - Integrity Checks

Perform an integrity check of [Assignment: organization-defined software, firmware, and information] [Selection (OneOrMore): at startup;at [selection to include security relevant event] ;[at least monthly] ] .

|  |
| --- |
| **SI-7(1) Control Summary Information** |
| Responsible Roles: Logging and Monitoring, Networking, SDL, Scanning |
| Parameter si-7.1\_prm\_1: software and information |
| Parameter si-7.1\_prm\_2: at deployment, continually, at least monthly |
| Parameter si-7.1\_prm\_3: |
| Parameter si-7.1\_prm\_4: |
| Parameter si-07.01\_odp.01: |
| Parameter si-07.01\_odp.02: |
| Parameter si-07.01\_odp.03: |
| Parameter si-07.01\_odp.04: |
| Parameter si-07.01\_odp.05: |
| Parameter si-07.01\_odp.06: |
| Parameter si-07.01\_odp.07: |
| Parameter si-07.01\_odp.08: |
| Parameter si-07.01\_odp.09: |
| Parameter si-07.01\_odp.10: |
| Parameter si-07.01\_odp.11: |
| Parameter si-07.01\_odp.12: |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SI-7(1) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for protecting software and information integrity for customer-deployed resources, including performing integrity checks of customer-defined software and information at customer-defined system transitional states (e.g., startup, restart, shutdown, abort), in response to customer-defined security-related events, or at a customer-defined frequency.  **Azure**  Azure software updates are reviewed for any unauthorized changes before entering the production environment as part of the Security Development Lifecycle (SDL) and Change and Release Management processes. Azure components have a set of runners which leverage information captured by Geneva Monitoring to run automated tests for checking the health of the components. Runners are configured to automatically generate alerts if any component health discrepancies are identified.  Azure also utilizes Azure Security Monitoring (ASM) for integrity scanning to reduce the risk of software components and devices potentially being tampered within the Azure environment. ASM has components that observe, analyze and report on security events continually in Azure environment. It complements the Azure security model by examining constraints that should always remain valid, which includes configuration settings.  Azure reassesses the integrity of software and information by monitoring of events reported via Windows Resource Protection (WRP) and File Integrity Monitoring (FIM). Network devices are monitored via Config Policy Verifier (CPV) and Config Change Reporter (CCR) in near-real time. WRP, FIM, CPV, and CCR are continuously scanning the environment for changes in near-real time that would constitute a change in the integrity of software in the system. |

### SI-7(2) - Automated Notifications of Integrity Violations

Employ automated tools that provide notification to [to include the ISSO and/or similar role within the organization] upon discovering discrepancies during integrity verification.

|  |
| --- |
| **SI-7(2) Control Summary Information** |
| Responsible Roles: Logging and Monitoring, Networking, SDL |
| Parameter si-07.02\_odp: Service Engineer Operations personnel |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SI-7(2) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for protecting software and information integrity for customer-deployed resources by employing automated tools that provide notification to customer-defined personnel/roles upon discovering discrepancies during integrity verification.  **Azure**  Azure software updates are thoroughly reviewed for any unauthorized changes before entering the production environments as part of the Security Development Lifecycle (SDL) and Change and Release Management processes. Any code changes must be reviewed and approved before they are deployed to the environment. Additionally, builds are digitally signed before they are deployed. If the integrity verification fails at deployment, the deployment operation fails, and the process needs to be started over. The deployment engine is configured to notify service teams upon discovery of discrepancies during integrity verification. Service teams are notified via email or the creation of DevOps tickets.  The Windows Server operating systems provide real-time file integrity validation, protection, and recovery of core system files that are installed as part of Windows or authorized Windows system updates. Windows Resource Protection (WRP) automatically detects and restores the original version of protected files if a program uses an unauthorized method to change those files.  WRP provides protection for system files using two mechanisms. The first mechanism runs in the background. This protection is triggered after WRP receives a directory change notification for a file in a protected directory. After WRP receives this notification, WRP determines which file was changed. If the file is protected, WRP looks up the file signature in a catalog file to determine if the new file is the correct version. If the file is not the correct version, WRP replaces the new file with the file from the system protected cache folder (if it is in the cache folder) or from the installation source. In addition to WRP, on demand validation and recovery of core Windows system files are provided using the System File Checker (sfc.exe) tool.  The Security File Integrity Monitoring (FIM) component consists of 2 elements:  \* System files protection provided by Windows Resource Protection (WRP) for Server baseline(s). This functionality is built into the operating system.  \* Critical file monitoring over and above that offered by WRP is provided by a combination of Local Security Policy settings for Windows Audit Object Access (WOA) together with the appropriate system access-control list (SACL) applied to the files designated as application-critical.  Both technologies write events to the event logs which are forwarded by an event forwarding tool and monitored by a security incident and event management tool. WRP is a real-time solution that performs scanning on a continuous basis.  **Network Devices**  Azure uses the Config Policy Verifier (CPV) and Config Change Reporter (CCR) tools to notify the Azure Networking team on unauthorized changes to network devices on a continuous basis. CPV and CCR automatically send alerts to Incident Management (IcM) regarding deviations of correct operations of security functions. CPV and CCR alert upon system startup and restart and continuously provides event monitoring and alerting to Azure Networking. CPV and CCR are near-real-time solutions that perform scanning on a continuous basis. |

### SI-7(5) - Automated Response to Integrity Violations

Automatically [Selection (OneOrMore): shut down the system;restart the system;implement [controls to be implemented automatically when integrity violations are discovered are defined (if selected);] ] when integrity violations are discovered.

|  |
| --- |
| **SI-7(5) Control Summary Information** |
| Responsible Roles: Logging and Monitoring, Networking, SDL |
| Parameter si-07.05\_odp.01: cancels deployment and notifies Service Engineer Operations personnel |
| Parameter si-07.05\_odp.02: |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SI-7(5) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for automatically shutting down or restarting customer-deployed resources, and/or implementing customer-defined security safeguards when integrity violations are discovered.  **Azure**  Azure provides alerts for integrity violations to the Security Response Team to use in case of suspected incidents. Shutting down the system would potentially cause operational issues including outages as a response to an integrity violation and expose the system to availability or denial of service risks. The Security Response Team investigates any instances of integrity violation that is suspected of being a security incident and respond according to their operating procedures.  Azure software updates are thoroughly reviewed for any unauthorized changes before entering the production environments as part of the Security Development Lifecycle (SDL) and Change and Release Management processes. Any code changes must be reviewed and approved before they are deployed to the environment. Additionally, builds are digitally signed before they are deployed. If the integrity verification fails at deployment, the deployment operation fails, and the process needs to be started over. The deployment engine is configured to notify service engineer personnel upon discovery of discrepancies during integrity verification. Service engineer personnel are notified via email or the creation of DevOps tickets.  **Servers**  The Windows Server operating systems provide real-time file integrity validation, protection, and recovery of core system files that are installed as part of Windows or authorized Windows system updates. Windows Resource Protection (WRP) automatically detects and restores the original version of protected files if a program uses an unauthorized method to change those files.  WRP provides protection for system files using two mechanisms. The first mechanism runs in the background. This protection is triggered after WRP receives a directory change notification for a file in a protected directory. After WRP receives this notification, WRP determines which file was changed. If the file is protected, WRP looks up the file signature in a catalog file to determine if the new file is the correct version. If the file is not the correct version, WRP replaces the new file with the file from the system protected cache folder (if it is in the cache folder) or from the installation source. In addition to WRP, on demand validation and recovery of core Windows system files are provided using the System File Checker (sfc.exe) tool.  **Network Devices**  Azure uses the Config Policy Verifier (CPV) and Config Change Reporter (CCR) tools to notify the Azure Networking team on unauthorized changes to network devices on a continuous basis. CPV and CCR automatically send alerts to Incident Management (IcM) regarding deviations of correct operations of security functions. CPV and CCR alert upon system startup and restart and continuously provides event monitoring and alerting to Azure Networking. CPV and CCR are near-real-time solutions that perform scanning on a continuous basis. |

### SI-7(7) - Integration of Detection and Response

Incorporate the detection of the following unauthorized changes into the organizational incident response capability: [security-relevant changes to the system are defined;].

|  |
| --- |
| **SI-7(7) Control Summary Information** |
| Responsible Roles: Logging and Monitoring |
| Parameter si-07.07\_odp: changes to operating system files, installation of software, privilege elevation |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SI-7(7) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for incorporating the detection of unauthorized customer-defined security-relevant changes to customer-deployed resources into the incident response capability.  **Azure**  **Servers**  In accordance with Microsoft Security Program Policy (MSPP), all software installed within Azure must have a valid signature. The Azure System Lockdown (AzSysLock) team uses AzSecPack to monitor for unexpected running software. This is defined as any software that is not signed using the appropriate signing certificates. AzSysLock sends alerts for service teams that are not properly using signed code. Additionally, for services running with AzSysLock in enforcement mode, which is currently an opt-in feature of AzSecPack, the binary does not run if it is not signed. Alerts for unsigned binaries running are created to service owners as a Severity 2 incident.  In addition, for servers, AzSecPack alerts on critical baseline changes.  **Network Devices**  The Config Policy Verifier (CPV) and Config Change Reporter (CCR) alerts on any changes not tied to a work ticket. |

### SI-7(15) - Code Authentication

Implement cryptographic mechanisms to authenticate the following software or firmware components prior to installation: [to include all software and firmware inside the boundary].

|  |
| --- |
| **SI-7(15) Control Summary Information** |
| Responsible Roles: Logging and Monitoring, SDL |
| Parameter si-07.15\_odp: all software and firmware inside the boundary |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SI-7(15) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for implementing cryptographic mechanisms to authenticate organization-defined software or firmware component prior to installation for customer-deployed resources.  **Azure**  The Microsoft Security Response Center monitors for the use of penetration testing tools installed within the Azure backend, as these have the potential to cause damage to the environment if used maliciously. Alerts are sent out to security teams if accounts are used maliciously. Refer to security controls of AU-2, SI-3, and SI-4 for further details.  Azure identifies software authorized to execute within Azure via configuration baselines and configuration scripts. Both baselines and scripts are version controlled and under configuration management. Only software included in a baseline or configuration script may be installed on Azure. Azure uses Azure Security Monitoring (ASM) and SCUBA to identify unauthorized software execution and alert appropriate personnel for further review.  In addition to the standard release processes as part of OneBranch processes which includes build release verification steps such as virus scanning, in accordance with Microsoft Security Program Policy (MSPP), all software installed within Azure must have a valid signature. The Azure System Lockdown (AzSysLock) team uses AzSecPack to monitor for unexpected running software. This is defined as any software that is not signed using the appropriate signing certificates. AzSysLock sends alerts for service teams that are not properly using signed code. Additionally, for services running with AzSysLock in enforcement mode, which is currently an opt-in feature of AzSecPack, the binary does not run if it is not signed. Alerts for unsigned binaries running are created to service owners as a Severity 2 incident.  For services running Azure Security Pack (AzSecPack), the OS security configuration baseline is also monitored for baseline violations, which are then reported to service owners through Incident Management (IcM) and/or Service 360 (S360) depending on the severity of the violation. Near real-time alerts include alerts for audit processing failures, such as system time changes or audit policy changes.  Additionally, virtual components within Azure are managed by the Fabric Controller (FC), which is the component that is used to create, monitor, restart, and destroy virtual machines. Overall VM and Azure Host/Native management coverage of AzSecPack is maintained by AzSecPack. |

## SI-8 Spam Protection

a. Employ spam protection mechanisms at system entry and exit points to detect and act on unsolicited messages; and

b. Update spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.

Guidance: When CSO sends email on behalf of the government as part of the business offering, Control Description should include implementation of Domain-based Message Authentication, Reporting & Conformance (DMARC) on the sending domain for outgoing messages as described in DHS Binding Operational Directive (BOD) 18-01. https://cyber.dhs.gov/bod/18-01/

Guidance: CSPs should confirm DMARC configuration (where appropriate) to ensure that policy=reject and the rua parameter includes reports@dmarc.cyber.dhs.gov. DMARC compliance should be documented in the SI-08 control implementation solution description, and list the FROM: domain(s) that will be seen by email recipients.

|  |
| --- |
| **SI-8 Control Summary Information** |
| Responsible Roles: Azure Compliance |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☒ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☒ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SI-8 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for employing spam protection at entry and exit points which detect and take action on unsolicited messages. Note: this control is only applicable to the customer if customer-deployed resources include an email server.  **Azure**  Currently, Azure does not host mail servers for its customers. |
| **Part B**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for updating spam protection in accordance with organization policy and procedures. Note: this control is only applicable to the customer if customer-deployed resources include an email server.  **Azure**  Currently, Azure does not host mail servers for its customers. |

### SI-8(2) - Automatic Updates

Automatically update spam protection mechanisms [the frequency at which to automatically update spam protection mechanisms is defined;].

|  |
| --- |
| **SI-8(2) Control Summary Information** |
| Responsible Roles: Azure Compliance |
| Parameter si-08.02\_odp: organization-defined frequency |
| Implementation Status (check all that apply):  ☐ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☒ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☒ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SI-8(2) What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for automatically updating spam protection. Note: this control is only applicable to the customer if customer-deployed resources include an email server.  **Azure**  Currently, Azure does not host mail servers for its customers. |

## SI-10 Information Input Validation

Check the validity of the following information inputs: [information inputs to the system requiring validity checks are defined;].

Requirement: Validate all information inputs and document any exceptions

|  |
| --- |
| **SI-10 Control Summary Information** |
| Responsible Roles: SDL |
| Parameter si-10: all information inputs |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SI-10 What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for information input validation for customer-deployed resources.  **Azure**  Azure follows system development methodology and security guidelines outlined in the Microsoft Security Policy (MSP), and service teams adhere to the Security Development Lifecycle (SDL) requirements described in the common Online Services Secure Coding procedure. The SDL process addresses requirements around input data validation within services. Thorough code reviews and testing are completed during the Verification Phase of the SDL prior to software being put into a production environment. The code reviews and testing check for a number of coding errors, including, but not limited to, SQL injection, format string vulnerabilities, XSS, integer arithmetic, command injection, and buffer overflow vulnerabilities, and ensures the services are able to handle such scenarios in a predictable manner. |

## SI-11 Error Handling

a. Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited; and

b. Reveal error messages only to [to include the ISSO and/or similar role within the organization].

|  |
| --- |
| **SI-11 Control Summary Information** |
| Responsible Roles: SDL |
| Parameter si-11(b): authorized service personnel and Azure users |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SI-11 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for generating error messages to provide information necessary for corrective actions without revealing information that could be exploited by adversaries for customer-deployed resources.  **Azure**  As part of the Security Development Lifecycle (SDL) process, service teams ensure that error messages do not contain sensitive information such as username and password combinations, attributes used to validate a password reset request, personally identifiable information excluding unique username identifiers provided as a normal part of a transactional record, biometric data or personal characteristics used to authenticate identity, sensitive financial records such as account numbers or access codes, content related to internal security functions such as private encryption keys, allowlist or deny list rules, or object permission attributes and settings. The error messages are generic in nature that provide limited information to assist the user in correcting the error. An example is “the username or password is incorrect” when there is an error logging into the application. |
| **Part B**  **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for revealing the error messages defined in SI-11.a to only customer-defined personnel or roles.  **Azure**  Except for error messages displayed to unauthenticated users, such as a login failure notification, error messages are shown only to authorized users and communicated across Azure only. Error messages are not accessible to external parties and only communicated to authorized users. |

## SI-12 Information Management and Retention

Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines and operational requirements.

|  |
| --- |
| **SI-12 Control Summary Information** |
| Responsible Roles: Privacy, CELA |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☐ Service Provider System Specific  ☒ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SI-12 What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for managing and retaining information within customer-deployed resources and information output from those resources in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.  **Azure**  Azure assets are retained as appropriate based on retention requirements set by Corporate Records Management and an asset’s classification or based on contractual requirements. The Microsoft Asset Classification Standard, Data Classification Standard, and Asset Protection Standard describe the minimum security requirements that Azure personnel must apply to information assets based on their classification, including Low Value Asset (LVA), Moderate Value Asset (MVA), and High Value Asset (HVA). The Corporate Document Retention Schedule describes which Microsoft documents must be kept and for how long. Microsoft guarantees retention of customer data for thirty (30) days after termination. All information is permanently deleted ninety (90) days after termination of service.  All Azure personnel responsible for managing and maintaining Azure assets ensure that assets are handled securely and provided with appropriate level of protection in accordance with the Asset Classification Standard, Data Classification Standard, and Asset Protection Standard. Microsoft assets are handled and retained in the following manner:  \* Information system documentation is accessible to Microsoft personnel via internal SharePoint sites. Individual service teams utilizing SharePoint are responsible for managing access to their own sites.  \* Operations assets are retained as appropriate based on retention requirements set by Corporate Records Management and the asset’s classification as document within the Asset Classification Standard and Asset Protection Standard.  \* Operations assets are disposed of in accordance with the asset’s retention requirements as set by Corporate Records Management. |

## SI-16 Memory Protection

Implement the following controls to protect the system memory from unauthorized code execution: [controls to be implemented to protect the system memory from unauthorized code execution are defined;].

|  |
| --- |
| **SI-16 Control Summary Information** |
| Responsible Roles: Azure Compliance |
| Parameter si-16: Windows protections, including No Execute, Address Space Layout Randomization, and Data Execution Prevention |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SI-16 What is the solution and how is it implemented?** |
| **Customer Responsibility**  For customers of IaaS and PaaS services, the customer is responsible for protecting customer-deployed resources from unauthorized code execution.  **Azure**  Azure uses Windows and Linux operating systems for its services. Both operating systems have protections in place for preventing code execution in restricted memory locations: No Execute (NX), Address Space Layout Randomization (ASLR), and Data Execution Prevention (DEP). Additionally, the Security Development Lifecycle (SDL) requires secure coding practices including explicit consideration for safe memory handling requirements.  See the following technical documentation for more information about the protections:  \* <https://docs.microsoft.com/en-us/windows/win32/memory/data-execution-prevention>  \* <https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-xp/bb457155(v=technet.10)>  \* <https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc771361(v=ws.10)>  \* <https://wiki.ubuntu.com/Security/Features#nx> |

# Supply Chain Risk Management (SR)

## SR-1 Policy and Procedures

a. Develop, document, and disseminate to [to include chief privacy and ISSO and/or similar role or designees]:

1. [Selection (OneOrMore): organization-level;mission/business process-level;system-level] supply chain risk management policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the supply chain risk management policy and the associated supply chain risk management controls;

b. Designate an [an official to manage the development, documentation, and dissemination of the supply chain risk management policy and procedures is defined;] to manage the development, documentation, and dissemination of the supply chain risk management policy and procedures; and

c. Review and update the current supply chain risk management:

1. Policy [at least annually] and following [events that require the current supply chain risk management policy to be reviewed and updated are defined;] ; and

2. Procedures [at least annually] and following [significant changes].

|  |
| --- |
| **SR-1 Control Summary Information** |
| Responsible Roles: SOP Team, Policy, Supply Chain |
| Parameter sr-1(a): all personnel |
| Parameter sr-01\_odp.01: |
| Parameter sr-01\_odp.02: |
| Parameter sr-01\_odp.03: a Microsoft-wide |
| Parameter sr-01\_odp.04: the Microsoft Information Risk Management Council (IRMC) organization |
| Parameter sr-01\_odp.05: at least annually |
| Parameter sr-01\_odp.06: significant changes |
| Parameter sr-01\_odp.07: at least annually |
| Parameter sr-01\_odp.08: significant changes |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SR-1 What is the solution and how is it implemented?** |
| **Part A1**  **Customer Responsibility**  The customer is responsible for developing, documenting, and disseminating supply chain risk management policy and procedures that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.  **Azure**  Azure addresses the supply chain risk management policy as part of the Microsoft security policies, of which there are two sets: the Microsoft Security Policy (MSP) that is applicable to all Microsoft personnel, and the Microsoft Security Program Policy (MSPP), which is applicable to all Microsoft personnel that have a responsibility for security. The Microsoft Information Risk Management Council (IRMC) is the governance body with review and approval responsibility for the MSP and MSPP. Within Azure, the MSPP specifically applies to all Microsoft personnel with security objectives such as designing, building, and operating Azure and across all information and processes used in the conduct of Microsoft business. All Azure personnel are accountable and responsible for complying with these guiding principles within their designated roles. The policy addresses the following:  \* Ownership of third-party relationships  \* Security Development Lifecycle (SDL)  \* Introduction of new hardware, software, or services  Additionally, the policy addresses the purpose, scope, roles, responsibilities, compliance requirements, and required coordination among the various Microsoft organizations that provide some level of support to all services. The policies indicate Microsoft management’s commitment and are a component of the risk management strategy which provides Azure personnel with a current set of clear and concise information security requirements.  The MSP is available to all Microsoft personnel on the Microsoft Policy website on the Microsoft intranet, and the MSPP and Security Standards are available through the Liquid tool, also on the Microsoft intranet. The Azure SOPs are stored in the Azure Security, Privacy & Compliance SharePoint site. This SharePoint site is accessible to all Azure personnel.  Service teams may supplement the Azure policies and procedures with offering-specific policies and procedures. Service-team-specific policies and procedures associated with access control are documented and stored within internal Azure SharePoint sites. Only personnel with authorized credentials, adequate levels of permission, legitimate need to know, and specific roles and responsibilities are given access to the service-team-specific policies or procedures. |
| **Part A2**  **Customer Responsibility**  The customer is responsible for procedures to facilitate the implementation of the access control policy and procedures and the associated access controls.  **Azure**  The Azure Access Control Standard Operating Procedure (SOP) implements the access control policy and associated controls and documents the following procedures:  \* Provisioning of Access  \* Modification and Review of Access Rights  \* Privilege Management  \* Inactive User Account Review  \* Separation of Duties  \* Remote Access Mechanisms  \* Session Control Parameters  Service teams may supplement the Azure policies and procedures with offering-specific policies and procedures. Service-team-specific policies and procedures associated with access control are documented and stored within internal Azure SharePoint sites. Only personnel with authorized credentials, adequate levels of permission, legitimate need to know, and specific roles and responsibilities are given access to the service-team-specific policies or procedures. |
| **Part B**  **Customer Responsibility**  The customer is responsible for designating an official to manage the development, documentation, and dissemination of the access control policy and procedures.  **Azure**  The Microsoft Information Risk Management Council (IRMC) organization is the governance body with approval responsibility for the Microsoft Security Policy (MSP) and Microsoft Security Program Policy (MSPP). The IRMC consists of representatives from security and risk management teams across Microsoft including Core Services Engineering and Operations (CSEO), Azure, and Global Security. The Customer Security and Trust: Security Engineering (CST-SE) organization manages the review and approval process and maintains the policies.  On an annual basis, the CST-SE conducts a line-by-line review of the MSP and MSPP. The Microsoft Security Policy (MSP) and Microsoft Security Program Policy (MSPP) Governance document describes each member’s role, types and frequency of review, escalation paths, approval process, and formal publishing procedures of the security policy. Throughout the year, if necessary, CST-SE may convene with the IRMC to conduct reviews after a significant review or change request. The approved policy update is published within the relevant tool on the Microsoft intranet. If service teams establish service-specific or team-specific policies, the respective service teams update the necessary policies at least annually. |
| **Part C1**  **Customer Responsibility**  The customer is responsible for reviewing and updating the current access control policy on a regular basis and following organization defined events.  **Azure**  The Azure team updates the Azure SOPs at least annually through a formal review process. If needed, the Azure team updates the SOP after a significant change affecting policy execution as well. If established, service-team-specific procedures are updated by their respective teams. The individual service teams review and update their respective SOPs at least annually and when required by a significant change. |
| **Part C2**  **Customer Responsibility**  The customer is responsible for reviewing and updating the current access control procedures on a regular basis and following organization defined events.  **Azure**  The Azure team updates the Azure SOPs at least annually through a formal review process. If needed, the Azure team updates the SOP after a significant change affecting policy execution as well. If established, service-team-specific procedures are updated by their respective teams. The individual service teams review and update their respective SOPs at least annually and when required by a significant change. |

## SR-2 Supply Chain Risk Management Plan

a. Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of the following systems, system components or system services: [systems, system components, or system services for which a supply chain risk management plan is developed are defined;];

b. Review and update the supply chain risk management plan [at least annually] or as required, to address threat, organizational or environmental changes; and

c. Protect the supply chain risk management plan from unauthorized disclosure and modification.

|  |
| --- |
| **SR-2 Control Summary Information** |
| Responsible Roles: Supply Chain |
| Parameter sr-02\_odp.01: organization-defined systems, system components, or system services |
| Parameter sr-02\_odp.02: at least annually |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SR-2 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  The customer is responsible for developing a plan for managing supply chain risks associated with research and development, design, and manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of customer-deployed resources.  **Azure**  Azure Supply Chain team has formulated a supply chain risk management plan document for managing supply chain risks associated with Azure cloud environments. The document is designed to address supply chain security and availability risks enabling Azure to comply against contractual and regulatory commitments. |
| **Part B**  **Customer Responsibility**  The customer is responsible for reviewing and updating supply chain risk management plan at customer-defined frequency and associated with customer-deployed resources.  **Azure**  Azure Supply Chain team works to ensure the supply chain risk management plan document is reviewed and updated on at least an annual basis or when there are significant changes requiring review. The document has a revision history table indicating when the document was last updated. |
| **Part C**  **Customer Responsibility**  The customer is responsible for protecting the supply chain risk management plan from unauthorized disclosure and modification for customer-deployed resources.  **Azure**  The Azure Supply Chain team leverages a protected and access-controlled website to house the supply chain risk management plan. Personnel who have the required job responsibilities have access to website and all other personnel don’t have access as role-based access control is enforced. |

### SR-2(1) - Establish SCRM Team

Establish a supply chain risk management team consisting of [the personnel, roles, and responsibilities of the supply chain risk management team are defined;] to lead and support the following SCRM activities: [supply chain risk management activities are defined;].

|  |
| --- |
| **SR-2(1) Control Summary Information** |
| Responsible Roles: Supply Chain |
| Parameter sr-02.01\_odp.01: organization-defined personnel, roles, and responsibilities |
| Parameter sr-02.01\_odp.02: organization-defined supply chain risk management activities |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SR-2(1) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for establishing a supply chain risk management team to support supply chain risk management activities for customer-deployed resources.  **Azure**  As part of Microsoft Supply Chain Security Program, Azure deploys a team responsible for leading and supporting supply chain risk management activities. The team members are introduced to industry-leading supply chain quality programs to support Azure cloud environments. |

## SR-3 Supply Chain Controls and Processes

a. Establish a process or processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of [the system or system component requiring a process or processes to identify and address weaknesses or deficiencies is defined;] in coordination with [supply chain personnel with whom to coordinate the process or processes to identify and address weaknesses or deficiencies in the supply chain elements and processes is/are defined;];

b. Employ the following controls to protect against supply chain risks to the system, system component, or system service and to limit the harm or consequences from supply chain-related events: [supply chain controls employed to protect against supply chain risks to the system, system component, or system service and to limit the harm or consequences from supply chain-related events are defined;] ; and

c. Document the selected and implemented supply chain processes and controls in [Selection (OneOrMore): security and privacy plans;supply chain risk management plan;[the document identifying the selected and implemented supply chain processes and controls is defined (if selected);] ] .

Requirement: CSO must document and maintain the supply chain custody, including replacement devices, to ensure the integrity of the devices before being introduced to the boundary.

|  |
| --- |
| **SR-3 Control Summary Information** |
| Responsible Roles: Supply Chain |
| Parameter sr-03\_odp.01: organization-defined system or system component |
| Parameter sr-03\_odp.02: organization-defined supply chain personnel |
| Parameter sr-03\_odp.03: organization-defined supply chain controls |
| Parameter sr-03\_odp.04: organization-defined document |
| Parameter sr-03\_odp.05: |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SR-3 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  The customer is responsible for establishing processes to identify and addresses weaknesses or deficiencies in supply chain elements and processes of customer-deployed resources in coordination with customer-defined supply chain personnel.  Azure  **Azure**  Azure has established a process to identify and addresses weaknesses or deficiencies in supply chain elements supporting Azure cloud environments as described below.  "One Microsoft" Supply Chain assurance efforts consist of numerous capabilities executing a corporate strategy that contributes to protecting Azure.  **Procurement**  During the initial supply chain phase, the Procurement team protects against supply chain threats by facilitating the creation of the purchase order to our suppliers ensuring consistency in approach.  <https://www.microsoft.com/en-us/procurement/supplier-contracting.aspx>  **Customer Operations**  Customer Operations performs routine business reviews with our suppliers representing the needs and concerns of all Azure business groups. This team also works to support Azure business groups on standards definition and service capability. A key function of this team is to protect against any threats posed by suppliers during manufacturing by ensuring adherence to standard supply chain methodologies and process adherence.  **Deployment Quality**  System integration or upon delivery of services to our Azure datacenters for deployment; Deployment Quality works to ensure final delivery of the system to the Azure business group is done on-time and free of defects. Working in conjunction with the Supply Chain Automation, these capabilities monitor performance metrics, capture business group feedback, and lead cross-functional Supply Chain.  **Supplier Relationship Management (SRM)**  As services move into the operations and maintenance phase of the life cycle, SRM protects Azure by managing and facilitating the supplier complaint process to drive root cause and corrective action within the suppliers’ supply chain. Supplier scorecards allow Azure to compare and visibly monitor the performance of our supply base utilizing a balanced scorecard approach.  **Spares**  Spares Management protects against supply chain threats by managing the determination and execution of obtaining spare components to support deployed devices within our Azure datacenters. Parts are spared to significantly reduce downtime of production equipment during a trouble-shooting scenario, helping to ensure site uptime for our business.  To ensure security of the supply chain and protection against threats, Azure uses well-established suppliers with a proven track record to secure supply chain management. In addition, these suppliers have established Service Level Agreements with critical providers to ensure that additional spare parts and maintenance activities are performed in a timely manner.  **Business Continuity**  Microsoft manages a comprehensive Continuity of Supply program with redundancies across Systems Integrators and components suppliers wherever possible. There is a team which drives continuous analysis of multi-source vs single source and end of life transitions for components across the Bill of Materials. Strategic purchases and inventories are held in an ongoing program to ensure supply of critical components and last time purchases. Supplier financial health is assessed routinely with risk assessments and deeper engagements on areas of concern.  **Asset Classification and Risk**  Assessments are determined by a "One Microsoft" team at initial infrastructure design and build to meet market/customer compliance boundary requirements. In addition, there are existing process for each service to provide its offering in each boundary. In addition, processes are in place for designated high integrity devices and services.  **Logistics**  Microsoft continues to increase assurance in the complex cloud global supply chain with next generation visibility by implementing a new global control tower capability, the next generation of supply chain visibility. The new capability delivers proactive intelligence on potential disruptions including weather, traffic, and global events, that allows Microsoft to notify our customer as the disruptions occur to adjust and deliver successfully. In addition, Microsoft is placing sensors on high value shipments with GPS capability supported by light and temperature detections at fifteen (15) minute tracking intervals.  **Validation**  Microsoft employs a capability to discover, configure, and validate in-rack hardware. The validation is executed at the original equipment manufacturer (OEM) prior to shipment and again at the Microsoft datacenter.  **Firmware**  Microsoft employs firmware source code guidance, reviews, and penetration tests to identify security vulnerabilities at the firmware level.  **Global Security Ecosystem Support**  Capabilities including Threat Intelligence, Digital Crime Unit, Cyber Defense Operations Center, and Service Security Teams, the Azure Red Team coordinated overt and covert activities to validate and strengthen the Global Azure and Specific Sovereign Infrastructures. In addition, the Third Party Assessment Organization (3PAO) penetration tests are part of the overall certifications.  **Industry Leadership**  The Microsoft Supply Chain Security program maintains industry-leading low loss levels across the various supply chains for the past five (5) years. Microsoft is Tier 3 certified with Customs Trade Partnership Against Terrorism (CTPAT), a Homeland Security / Customs and Border Protection program, and Authorized Economic Operator (AEO) certified in India, pending Australia.  **Global Leadership and Partnerships**  Microsoft members maintain leadership roles in the Transported Asset Protection Association (TAPA) and the Alliance for Gray Market and Counterfeit Abatement (AGMA). In addition, Microsoft maintains active representation in the European Union, North Atlantic Treaty Organization, and World Trade Organization. |
| **Part B**  **Customer Responsibility**  The customer is responsible for employing controls to protect against supply chain risk to the system, system component, or system service and to limit harm or consequences from supply chain-related events for customer-deployed resources.  **Azure**  Azure has deployed supply chain controls described in SR-3 control part a above. The controls are designed to protect against supply chain risks to Azure cloud environments and to limit harm or consequences from supply chain related events. |
| **Part C**  **Customer Responsibility**  The customer is responsible for documenting the selected and implemented supply chain processes and controls in security, privacy, or supply chain management plan document for customer-deployed resources.  **Azure**  Azure has documented the supply chain processes and controls described in SR-3 control above as part of Microsoft Security Policy (MSP) and Microsoft Security Program Policy (MSPP), and Supply Chain Risk Management Plan documents. |

## SR-5 Acquisition Strategies, Tools, and Methods

Employ the following acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risks: [acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risks are defined;].

|  |
| --- |
| **SR-5 Control Summary Information** |
| Responsible Roles: CELA, Supply Chain |
| Parameter sr-5: organization-defined acquisition strategies, contract tools, and procurement methods |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SR-5 What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for employing acquisition strategies, contract tools, and procurement methods for customer-deployed resources to protect against supply chain risks.  The customer is responsible for employing organization-defined tailored acquisition strategies, contract tools, and procurement methods for the purchase of the information system, system component, or information system service from suppliers.  **Azure**  Azure has established the following supply chain acquisition strategies, contract tools, and procurement methods to support Azure cloud environments.  "One Microsoft" Supply Chain assurance efforts consist of numerous capabilities executing a corporate strategy that contributes to protecting Azure.  **Procurement**  During the initial supply chain phase, the Procurement team protects against supply chain threats by facilitating the creation of the purchase order to our suppliers ensuring consistency in approach.  <https://www.microsoft.com/en-us/procurement/supplier-contracting.aspx>  **Customer Operations**  Customer Operations performs routine business reviews with our suppliers representing the needs and concerns of all Azure business groups. This team also works to support Azure business groups on standards definition and service capability. A key function of this team is to protect against any threats posed by suppliers during manufacturing by ensuring adherence to standard supply chain methodologies and process adherence.  **Deployment Quality**  System integration or upon delivery of services to our Azure datacenters for deployment; Deployment Quality works to ensure final delivery of the system to the Azure business group is done on-time and free of defects. Working in conjunction with the Supply Chain Automation, these capabilities monitor performance metrics, capture business group feedback, and lead cross-functional Supply Chain.  **Supplier Relationship Management (SRM)**  As services move into the operations and maintenance phase of the life cycle, SRM protects Azure by managing and facilitating the supplier complaint process to drive root cause and corrective action within the suppliers’ supply chain. Supplier scorecards allow Azure to compare and visibly monitor the performance of our supply base utilizing a balanced scorecard approach.  **Spares**  Spares Management protects against supply chain threats by managing the determination and execution of obtaining spare components to support deployed devices within our Azure datacenters. Parts are spared to significantly reduce downtime of production equipment during a trouble-shooting scenario, helping to ensure site uptime for our business.  To ensure security of the supply chain and protection against threats, Azure uses well-established suppliers with a proven track record to secure supply chain management. In addition, these suppliers have established Service Level Agreements with critical providers to ensure that additional spare parts and maintenance activities are performed in a timely manner.  **Business Continuity**  Microsoft manages a comprehensive Continuity of Supply program with redundancies across Systems Integrators and components suppliers wherever possible. There is a team which drives continuous analysis of multi-source vs single source and end of life transitions for components across the Bill of Materials. Strategic purchases and inventories are held in an ongoing program to ensure supply of critical components and last time purchases. Supplier financial health is assessed routinely with risk assessments and deeper engagements on areas of concern.  **Asset Classification and Risk**  Assessments are determined by a "One Microsoft" team at initial infrastructure design and build to meet market/customer compliance boundary requirements. In addition, there are existing process for each service to provide its offering in each boundary. In addition, processes are in place for designated high integrity devices and services.  **Logistics**  Microsoft continues to increase assurance in the complex cloud global supply chain with next generation visibility by implementing a new global control tower capability, the next generation of supply chain visibility. The new capability delivers proactive intelligence on potential disruptions including weather, traffic, and global events, that allows Microsoft to notify our customer as the disruptions occur to adjust and deliver successfully. In addition, Microsoft is placing sensors on high value shipments with GPS capability supported by light and temperature detections at fifteen (15) minute tracking intervals.  **Validation**  Microsoft employs a capability to discover, configure, and validate in-rack hardware. The validation is executed at the original equipment manufacturer (OEM) prior to shipment and again at the Microsoft datacenter.  **Firmware**  Microsoft employs firmware source code guidance, reviews, and penetration tests to identify security vulnerabilities at the firmware level.  **Global Security Ecosystem Support**  Capabilities including Threat Intelligence, Digital Crime Unit, Cyber Defense Operations Center, and Service Security Teams, the Azure Red Team coordinated overt and covert activities to validate and strengthen the Global Azure and Specific Sovereign Infrastructures. In addition, the Third Party Assessment Organization (3PAO) penetration tests are part of the overall certifications.  **Industry Leadership**  The Microsoft Supply Chain Security program maintains industry-leading low loss levels across the various supply chains for the past five (5) years. Microsoft is Tier 3 certified with Customs Trade Partnership Against Terrorism (CTPAT), a Homeland Security / Customs and Border Protection program, and Authorized Economic Operator (AEO) certified in India, pending Australia.  **Global Leadership and Partnerships**  Microsoft members maintain leadership roles in the Transported Asset Protection Association (TAPA) and the Alliance for Gray Market and Counterfeit Abatement (AGMA). In addition, Microsoft maintains active representation in the European Union, North Atlantic Treaty Organization, and World Trade Organization. |

## SR-6 Supplier Assessments and Reviews

Assess and review the supply chain-related risks associated with suppliers or contractors and the system, system component, or system service they provide [at least annually].

Requirement: CSOs must ensure that their supply chain vendors build and test their systems in alignment with NIST SP 800-171 or a commensurate security and compliance framework. CSOs must ensure that vendors are compliant with physical facility access and logical access controls to supplied products.

|  |
| --- |
| **SR-6 Control Summary Information** |
| Responsible Roles: Azure Compliance, Supply Chain |
| Parameter sr-6: organization-defined frequency |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SR-6 What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for assessing and reviewing the supply chain related risks associated with suppliers or contractors and the system, system component, or system service they provide for customer-deployed resources at a defined frequency.  **Azure**  "One Microsoft" Supply Chain assurance efforts consist of numerous capabilities executing a corporate strategy that contributes to protecting Azure. The following efforts take place for Azure to assess and review the supply chain-related risks associated with supplier or contacts and Azure components they provide on an at least annual cadence.  **Procurement**  During the initial supply chain phase, the Procurement team protects against supply chain threats by facilitating the creation of the purchase order to our suppliers ensuring consistency in approach.  <https://www.microsoft.com/en-us/procurement/supplier-contracting.aspx>  **Customer Operations**  Customer Operations performs routine business reviews with our suppliers representing the needs and concerns of all Azure business groups. This team also works to support Azure business groups on standards definition and service capability. A key function of this team is to protect against any threats posed by suppliers during manufacturing by ensuring adherence to standard supply chain methodologies and process adherence.  **Deployment Quality**  System integration or upon delivery of services to our Azure datacenters for deployment; Deployment Quality works to ensure final delivery of the system to the Azure business group is done on-time and free of defects. Working in conjunction with the Supply Chain Automation, these capabilities monitor performance metrics, capture business group feedback, and lead cross-functional Supply Chain.  **Supplier Relationship Management (SRM)**  As services move into the operations and maintenance phase of the life cycle, SRM protects Azure by managing and facilitating the supplier complaint process to drive root cause and corrective action within the suppliers’ supply chain. Supplier scorecards allow Azure to compare and visibly monitor the performance of our supply base utilizing a balanced scorecard approach.  **Spares**  Spares Management protects against supply chain threats by managing the determination and execution of obtaining spare components to support deployed devices within our Azure datacenters. Parts are spared to significantly reduce downtime of production equipment during a trouble-shooting scenario, helping to ensure site uptime for our business.  To ensure security of the supply chain and protection against threats, Azure uses well-established suppliers with a proven track record to secure supply chain management. In addition, these suppliers have established Service Level Agreements with critical providers to ensure that additional spare parts and maintenance activities are performed in a timely manner.  **Business Continuity**  Microsoft manages a comprehensive Continuity of Supply program with redundancies across Systems Integrators and components suppliers wherever possible. There is a team which drives continuous analysis of multi-source vs single source and end of life transitions for components across the Bill of Materials. Strategic purchases and inventories are held in an ongoing program to ensure supply of critical components and last time purchases. Supplier financial health is assessed routinely with risk assessments and deeper engagements on areas of concern.  **Asset Classification and Risk**  Assessments are determined by a "One Microsoft" team at initial infrastructure design and build to meet market/customer compliance boundary requirements. In addition, there are existing process for each service to provide its offering in each boundary. In addition, processes are in place for designated high integrity devices and services.  **Logistics**  Microsoft continues to increase assurance in the complex cloud global supply chain with next generation visibility by implementing a new global control tower capability, the next generation of supply chain visibility. The new capability delivers proactive intelligence on potential disruptions including weather, traffic, and global events, that allows Microsoft to notify our customer as the disruptions occur to adjust and deliver successfully. In addition, Microsoft is placing sensors on high value shipments with GPS capability supported by light and temperature detections at fifteen (15) minute tracking intervals.  **Validation**  Microsoft employs a capability to discover, configure, and validate in-rack hardware. The validation is executed at the original equipment manufacturer (OEM) prior to shipment and again at the Microsoft datacenter.  **Firmware**  Microsoft employs firmware source code guidance, reviews, and penetration tests to identify security vulnerabilities at the firmware level.  **Global Security Ecosystem Support**  Capabilities including Threat Intelligence, Digital Crime Unit, Cyber Defense Operations Center, and Service Security Teams, the Azure Red Team coordinated overt and covert activities to validate and strengthen the Global Azure and Specific Sovereign Infrastructures. In addition, the Third Party Assessment Organization (3PAO) penetration tests are part of the overall certifications.  **Industry Leadership**  The Microsoft Supply Chain Security program maintains industry-leading low loss levels across the various supply chains for the past five (5) years. Microsoft is Tier 3 certified with Customs Trade Partnership Against Terrorism (CTPAT), a Homeland Security / Customs and Border Protection program, and Authorized Economic Operator (AEO) certified in India, pending Australia.  **Global Leadership and Partnerships**  Microsoft members maintain leadership roles in the Transported Asset Protection Association (TAPA) and the Alliance for Gray Market and Counterfeit Abatement (AGMA). In addition, Microsoft maintains active representation in the European Union, North Atlantic Treaty Organization, and World Trade Organization. |

## SR-8 Notification Agreements

Establish agreements and procedures with entities involved in the supply chain for the system, system component, or system service for the [Selection (OneOrMore): notification of supply chain compromises;[information for which agreements and procedures are to be established are defined (if selected);] ] .

Requirement: CSOs must ensure and document how they receive notifications from their supply chain vendor of newly discovered vulnerabilities including zero-day vulnerabilities.

|  |
| --- |
| **SR-8 Control Summary Information** |
| Responsible Roles: CELA, Supply Chain |
| Parameter sr-08\_odp.01: notification of supply chain compromises and results of assessment or audits |
| Parameter sr-08\_odp.02: |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SR-8 What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for establishing agreements and procedures with entities involved in the supply chain for customer-deployed resources to notify against supply chain compromise and results of assessments or audits for customer-defined information.  **Azure**  As part of Microsoft Supply Chain Security Program, Azure deploys a team responsible for leading and supporting supply chain risk management activities. The team members are introduced to industry-leading supply chain quality programs to support Azure cloud environments. The team members have established agreements and procedures with various Azure partner teams of supply chain such as Azure Security, Azure Federal Compliance, and CELA teams for the notification of supply chain compromises and findings that are a result of assessments. If findings are identified, stakeholders of Azure cloud environments are notified through the approval of CELA on communication plans. Remediation plans for supply chain compromises or findings during assessments are formulated to track until implementation by team members who lead and support supply chain risk management activities. |

## SR-9 Tamper Resistance and Detection

Implement a tamper protection program for the system, system component, or system service.

Requirement: CSOs must ensure vendors provide authenticity of software and patches supplied to the service provider including documenting the safeguards in place.

|  |
| --- |
| **SR-9 Control Summary Information** |
| Responsible Roles: Datacenter Hosting, Supply Chain |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SR-9 What is the solution and how is it implemented?** |

### SR-9(1) - Multiple Stages of System Development Life Cycle

Employ anti-tamper technologies, tools, and techniques throughout the system development life cycle.

|  |
| --- |
| **SR-9(1) Control Summary Information** |
| Responsible Roles: SDL |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SR-9(1) What is the solution and how is it implemented?** |

## SR-10 Inspection of Systems or Components

Inspect the following systems or system components [Selection (OneOrMore): at random;at [frequency at which to inspect systems or system components is defined (if selected);] ;upon [indications of the need for an inspection of systems or system components are defined (if selected);] ] to detect tampering: [systems or system components that require inspection are defined;].

|  |
| --- |
| **SR-10 Control Summary Information** |
| Responsible Roles: Datacenter Hosting, Supply Chain |
| Parameter sr-10\_odp.01: organization-defined frequency |
| Parameter sr-10\_odp.02: organization-defined systems or system components |
| Parameter sr-10\_odp.03: |
| Parameter sr-10\_odp.04: |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SR-10 What is the solution and how is it implemented?** |

## SR-11 Component Authenticity

a. Develop and implement anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the system; and

b. Report counterfeit system components to [Selection (OneOrMore): source of counterfeit component;[external reporting organizations to whom counterfeit system components are to be reported is/are defined (if selected);] ;[personnel or roles to whom counterfeit system components are to be reported is/are defined (if selected);] ] .

Requirement: CSOs must ensure that their supply chain vendors provide authenticity of software and patches and the vendor must have a plan to protect the development pipeline.

|  |
| --- |
| **SR-11 Control Summary Information** |
| Responsible Roles: Policy, Supply Chain |
| Parameter sr-11\_odp.01: organization-defined external reporting organizations |
| Parameter sr-11\_odp.02: |
| Parameter sr-11\_odp.03: |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SR-11 What is the solution and how is it implemented?** |
| **Part A**  **Customer Responsibility**  The customer is responsible for developing and implementing anti-counterfeit policy and procedures in order to detect and prevent counterfeit components.  **Azure**  Azure has processes in place to prevent and detect counterfeit components from entering the information system. As preventive measures, Azure must follow the Microsoft corporate procurement process. Azure sources hardware and software only through original equipment manufacturer (OEM) suppliers and their certified distribution partners that have been approved by the procurement process. Within the agreements with suppliers of hardware and software there are security provisions to ensure the security of the supply chain and protection against threats such as counterfeit components. Additionally, for its infrastructure services Azure maintains authoritative lists of approved software through its Definitive Software Library (DSL) as well as IPAK images. This ensures that software and updates are from approved sources.  As a detective measure, Azure implements vulnerability scanning for the Azure environment by actively scanning all server operating systems, network devices, web applications, and databases in the Azure inventory with authenticated scans.  Risk Protective Services (RPS), of which Anti-Piracy Services (APS) is a part, manages Microsoft’s Supply Chain Security program for its traditional Manufacturing and Digital Supply Chain, including, but not limited to: device manufacturing (Xbox, Surface, accessories); software manufacturing both physical and digital, distribution of products, secure print (COA, Xbox Live, Skype, Office cards), digital distribution, OEM, Azure, and more.  The technologies these products utilize, as well as telemetry data on key usage and investigations of abuse, and counterfeit.  All these suppliers are required to adhere to Microsoft policies by contract.  APS partners with other teams within Microsoft to insure suppliers are secure both physically and digitally – IRSM (IT), DCU (Digital Crimes Unit), CCR (Cyber Crimes Unit), Global Security (Microsoft assets and people), Azure supply chain, WDG Security (leak prevention and new product introduction and investigations).   APS crosses all lines of business and channels at Microsoft.  The Supply Chain Security (SCS) program manages Microsoft’s tier 3 program with Customs Trade Partnership Against Terrorism (CTPAT), a Homeland Security / Customs and Border Protection program.  SCS manages supplier security requirements, best practices and compliance inspections throughout Microsoft physical and digital supply chains.  The requirements are reviewed annually against industry best practices and updated.  Risk analysis of the Microsoft global supply chain is performed annually.  Microsoft continues to increase assurance in the complex cloud global supply chain with next generation visibility by implementing a new global control tower capability, the next generation of supply chain visibility. The new capability delivers proactive intelligence on potential disruptions including weather, traffic, and global events, that allows Microsoft to notify our customer as the disruptions occur to adjust and deliver successfully. In addition, Microsoft is placing sensors on high value shipments with GPS capability supported by light and temperature detections at fifteen (15) minute tracking intervals.  Microsoft employs a capability to discover, configure, and validate in-rack hardware. The validation is executed at the OEM prior to shipment and again at the Microsoft datacenter.  Microsoft employs firmware source code guidance, reviews and penetration tests to identify security vulnerabilities at the firmware level.  Microsoft capabilities including Threat Intelligence, Digital Crime Unit, Cyber Defense Operations Center, and Service Security Teams, the Azure Red Team utilize coordinated overt and covert activities to validate and strengthen the Global Azure and Specific Sovereign Infrastructures. In addition, Third Party Assessment Organization (3PAO) penetration tests are part of the overall certifications. |
| **Part B**  **Customer Responsibility**  The customer is responsible for reporting counterfeit information system components to the source of the counterfeit components, customer-defined external reporting organizations, and/or customer-defined personnel/roles.  **Azure**  Reports of counterfeit information system components follows the incident handling procedures. In the event a counterfeit incident impacts Azure assets or services requiring customer notification, the Security Response Team coordinates with the service team to notify the customer and USCYBERCOM. |

### SR-11(1) - Anti-counterfeit Training

Train [personnel or roles requiring training to detect counterfeit system components (including hardware, software, and firmware) is/are defined;] to detect counterfeit system components (including hardware, software, and firmware).

|  |
| --- |
| **SR-11(1) Control Summary Information** |
| Responsible Roles: Supply Chain |
| Parameter sr-11.01\_odp: organization-defined personnel or roles |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SR-11(1) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for training personnel to detect counterfeit information system components supporting customer-deployed resources.  **Azure**  The Microsoft Supply Chain Security program maintains industry-leading quality programs whereby Microsoft members maintain leadership roles in the Transported Asset Protection Association (TAPA) and the Alliance for Gray Market and Counterfeit Abatement (AGMA). In addition, Microsoft maintains active representation in the European Union, North Atlantic Treaty Organization, and World Trade Organization. Personnel supporting the program are trained under the curriculum programs identified in AT control family. All members of software development teams receive appropriate training to stay informed about security basics and recent trends in security. Individuals who develop software programs are required to complete at least one security training course in person or online each year. Security training can help ensure software is created with security in mind and can also help development teams stay current on security issues. Project team members are strongly encouraged to seek additional security and privacy education that is appropriate to their needs or products.  Azure service teams maintain, secure, manage, and store information system documentation, including documentation regarding:  \* Secure configuration, installation, and operation of the information system;  \* Effective use and maintenance of security features/functions; and  \* Known vulnerabilities regarding configuration and use of administrative (i.e., elevated) functions  This documentation is stored in each service team’s SharePoint site or STRIKE Central and is made available to service team members. Review of relevant documentation is part of initial and ongoing training activities held at least annually. |

### SR-11(2) - Configuration Control for Component Service and Repair

Maintain configuration control over the following system components awaiting service or repair and serviced or repaired components awaiting return to service: [all].

|  |
| --- |
| **SR-11(2) Control Summary Information** |
| Responsible Roles: Datacenter Hosting |
| Parameter sr-11.02\_odp: |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☒ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SR-11(2) What is the solution and how is it implemented?** |
| **Customer Responsibility**  The customer is responsible for maintaining configuration control over customer-controlled information system components awaiting service or repair and serviced or repaired.  **Azure**  Information system components that make up Azure cloud environments consist of physical digital media hardware and logical software. Both digital media and logical software components of Azure cloud environments are housed in Azure datacenters deployed in United States geographic locations.  Datacenter Management (DCM) and Critical Environment (CE) teams implement configuration control for digital media hardware awaiting service or repair and serviced or repaired at Azure datacenters. The digital media hardware changes are tested and documented for investigation purposes.  For logical software, Azure service teams deploy configuration control on information system components awaiting service or repair and serviced or repaired. Changes are conducted in a separate development/test environment, are subject to testing with defined pass rates, peer review to enforce separation of duties, and are implemented into production via Safe Deployment Practices (SDP). Changes are documented for investigation purposes. |

## SR-12 Component Disposal

Dispose of [data, documentation, tools, or system components to be disposed of are defined;] using the following techniques and methods: [techniques and methods for disposing of data, documentation, tools, or system components are defined;].

|  |
| --- |
| **SR-12 Control Summary Information** |
| Responsible Roles: Datacenter Hosting |
| Parameter sr-12\_odp.01: organization-defined data, documentation, tools, or system components |
| Parameter sr-12\_odp.02: organization-defined techniques and methods |
| Implementation Status (check all that apply):  ☒ Implemented  ☐ Partially implemented  ☐ Planned  ☐ Alternative implementation  ☐ Not applicable |
| Control Origination (check all that apply):  ☐ Service Provider Corporate  ☒ Service Provider System Specific  ☐ Service Provider Hybrid (Corporate and System Specific)  ☐ Configured by Customer (Customer System Specific)  ☐ Provided by Customer (Customer System Specific)  ☐ Shared (Service Provider and Customer Responsibility)  ☐ Inherited from pre-existing Authorization |

|  |
| --- |
| **SR-12 What is the solution and how is it implemented?** |
| **Azure**  In Azure datacenters , Azure digital media is sanitized using approved tools and in compliance with customer requirements, including NIST Special Publication 800-88 Revision 1 prior to being reused. Non-digital media is not used by Azure in the datacenter environment.  All data bearing devices (DBDs) used by Azure are shredded by an approved ITAD Vendor or customer per customer standards on site. No DBDs leave the Azure datacenters . If hardware is considered volatile and deemed returnable to the supplier, it is shipped out via the standard RMA process as outlined in the Sparing and RMA Strategy. For assets requiring destruction, Azure utilizes onsite asset destruction services. |