FedRAMP System Security Plan (SSP)

|  |
| --- |
|  |



Microsoft Corporation

Office 365 MultiTenant (MT)

Version 6.01

August 31, 2018

Controlled Unclassified Information

System Security Plan

Prepared by

| Identification of Organization that Prepared this Document | | |
| --- | --- | --- |
|  | Organization Name | First Information Technology Services, Inc. |
| Street Address | 777 108th Ave. NE |
| Suite/Room/Building | 1850 |
| City, State Zip | Bellevue, Washington 98004 |

Prepared for

| Identification of Cloud Service Provider | | |
| --- | --- | --- |
|  | Organization Name | Microsoft Corporation |
| Street Address | 1 Microsoft Way |
| Suite/Room/Building | Building 31 |
| City, State Zip | Redmond, WA 98052 |

Revision History

| Date | Description | Version of SSP | Author |
| --- | --- | --- | --- |
| 1/9/2015 | Minor changes for beginning of audit; began detailed change log going forward | 2.03 | FITS |
| 6/5/2015 | Adjusted for Changes made in MSFT Environment and audit results | 2.04 | FITS |
| 7/6/2015 | Updated Control Summary Information for controls with customer responsibility & minor edits | 2.05 | FITS |
| 8/3/2015 | Updated Control Implementation Details for controls based on POA&M updates, and additional minor edits | 2.06 | FITS |
| 8/4/2015 | Updated Control Implementation Details for controls based on POA&M updates, and additional minor edits | 2.07 | FITS |
| 8/11/2015 | Updated Control Implementation Details & minor edits | 2.08 | FITS |
| 9/8/2015 | Updated Control Summary Information for controls with customer responsibility & minor edits | 2.09 | FITS |
| 12/14/2015 | Major revision for annual assessment; updated system description and reviewed and updated all control implementations. | 3.00 | FITS |
| 5/13/2016 | Minor revision to incorporate updates from FY16 FedRAMP audit | 3.01 | FITS |
| 7/28/2016 | Minor revision to include updates from FY16 FedRAMP SAR | 3.02 | FITS |
| 2/21/2017 | Major revision for annual assessment; updated system description and reviewed and updated all control implementations. | 4.00 | FITS |
| 9/30/17 | - Major revision for Delta Audit: added Microsoft Teams (MSTeams), Object Store (OStore), and Outlook Mobile (OLM) as new workloads.  - Added Atlassian to section 11 for system interconnections, and all relevant controls.  - Removed Level 3 Communications from section 11 and all relevant controls. | 5.00 | FITS |
| 10/27/17 | Added DFDs for MS Teams, Object Store, and Outlook Mobile | 5.01 | FITS |
| 1/12/17 | Minor revisions to include updates from FY 17 Delta Audit | 5.02 | FITS |
| 3/16/2018 | Major revision for annual assessment; updated system description and reviewed and updated all control implementations. | 6.0 | Microsoft |
| 8/31/2018 | Updated for Spring 2018 SAR and minor edits | 6.01 | Microsoft |

How to contact us

For questions about FedRAMP, or for technical questions about this document including how to use it, contact info@FedRAMP.gov

For more information about the FedRAMP project, see www.FedRAMP.gov

Table of Contents

[1. Information System Name/Title 1](#_Toc507670141)

[2. Information System Categorization 1](#_Toc507670142)

[2.1. Information Types 1](#_Toc507670143)

[2.2. Security Objectives Categorization (FIPS 199) 3](#_Toc507670144)

[2.3. E-Authentication Determination 4](#_Toc507670145)

[3. Information System Owner 4](#_Toc507670146)

[4. Authorizing Official 4](#_Toc507670147)

[5. Other Designated Contacts 4](#_Toc507670148)

[6. Assignment of Security Responsibility 5](#_Toc507670149)

[7. Information System Operational Status 6](#_Toc507670150)

[8. Information System Type 6](#_Toc507670151)

[8.1. Cloud Service Models 6](#_Toc507670152)

[8.2. Cloud Deployment Models 7](#_Toc507670153)

[8.3. Leveraged Authorizations 7](#_Toc507670154)

[9. General System Description 8](#_Toc507670155)

[9.1. System Function or Purpose 8](#_Toc507670156)

[9.1.1. Service Summary 8](#_Toc507670157)

[9.1.2. Security Overview 9](#_Toc507670158)

[9.1.3. Active Directory Federation Service (ADFS) 10](#_Toc507670159)

[9.1.4. Office 365 MT vs Office 365 GCC 10](#_Toc507670160)

[9.2. Information System Components and Boundaries 12](#_Toc507670161)

[9.3. Types of Users 14](#_Toc507670162)

[9.4. Network Architecture 16](#_Toc507670163)

[9.5. Service Description 17](#_Toc507670164)

[9.5.1. Exchange Online (EXO) 17](#_Toc507670165)

[9.5.2. SharePoint Online (SPO) 18](#_Toc507670166)

[9.5.3. Skype for Business (SFB) 20](#_Toc507670167)

[9.5.4. Information Protection (IP) 22](#_Toc507670168)

[9.5.5. Office Online (WAC) 23](#_Toc507670169)

[9.5.6. Security Workload Environment (SWE) 24](#_Toc507670170)

[9.5.7. Domain Name Service (DNS) 25](#_Toc507670171)

[9.5.8. Office 365 Suite User Experience (SUE) 26](#_Toc507670172)

[9.5.9. Office Service Infrastructure (OSI) 27](#_Toc507670173)

[9.5.10. Azure Active Directory (AAD) 29](#_Toc507670174)

[9.5.11. Microsoft Teams (MSTeams) 30](#_Toc507670175)

[9.5.12. Bing 31](#_Toc507670176)

[9.5.13. Outlook Mobile (OLM) 32](#_Toc507670177)

[9.5.14. Delve 33](#_Toc507670178)

[10. System Environment And Inventory 34](#_Toc507670179)

[10.1. Data Flow 35](#_Toc507670180)

[10.2. Ports, Protocols, and Services 35](#_Toc507670181)

[11. System Interconnections 36](#_Toc507670182)

[12. Laws, Regulations, Standards and Guidance 37](#_Toc507670183)

[12.1. Applicable Laws and Regulations 37](#_Toc507670184)

[12.2. Applicable Standards and Guidance 37](#_Toc507670185)

[13. Minimum Security Controls 37](#_Toc507670186)

[13.1. Access Control (AC) 47](#_Toc507670187)

[AC-1 Access Control Policy and Procedures Requirements (L) (M) 47](#_Toc507670188)

[AC-2 Account Management (L) (M) 49](#_Toc507670189)

[AC-2 (1) Control Enhancement (M) (H) 57](#_Toc507670190)

[AC-2 (2) Control Enhancement (M) 59](#_Toc507670191)

[AC-2 (3) Control Enhancement (M) 60](#_Toc507670192)

[AC-2 (4) Control Enhancement (M) 62](#_Toc507670193)

[AC-2 (5) Control Enhancement (M) 64](#_Toc507670194)

[AC-2 (7) Control Enhancement (M) 65](#_Toc507670195)

[AC-2 (9) Control Enhancement (M) 68](#_Toc507670196)

[AC-2 (10) Control Enhancement (M) (H) 69](#_Toc507670197)

[AC-2 (12) Control Enhancement (M) 70](#_Toc507670198)

[AC-3 Access Enforcement (L) (M) (H) 71](#_Toc507670199)

[AC-4 Information Flow Enforcement (M) (H) 73](#_Toc507670200)

[AC-4 (21) Control Enhancement (M) (H) 75](#_Toc507670201)

[AC-5 Separation of Duties (M) (H) 76](#_Toc507670202)

[AC-6 Least Privilege (M) (H) 79](#_Toc507670203)

[AC-6 (1) Control Enhancement (M) 81](#_Toc507670204)

[AC-6 (2) Control Enhancement (M) (H) 83](#_Toc507670205)

[AC 6 (5) Control Enhancement (M) (H) 85](#_Toc507670206)

[AC-6 (9) Control Enhancement (M) (H) 86](#_Toc507670207)

[AC-6 (10) Control Enhancement (M) (H) 87](#_Toc507670208)

[AC-7 Unsuccessful Login Attempts (L) (M) 88](#_Toc507670209)

[AC-8 System Use Notification (L) (M) (H) 90](#_Toc507670210)

[AC-10 Concurrent Session Control (M) (H) 97](#_Toc507670211)

[AC-11 Session Lock (M) (H) 98](#_Toc507670212)

[AC-11 (1) Control Enhancement (M) (H) 99](#_Toc507670213)

[AC-12 Session Termination (M) (H) 101](#_Toc507670214)

[AC-14 Permitted Actions without Identification or Authentication (L) (M) (H) 102](#_Toc507670215)

[AC-17 Remote Access (L) (M) (H) 104](#_Toc507670216)

[AC-17 (1) Control Enhancement (M) (H) 106](#_Toc507670217)

[AC-17 (2) Control Enhancement (M) (H) 108](#_Toc507670218)

[AC-17 (3) Control Enhancement (M) (H) 110](#_Toc507670219)

[AC-17 (4) Control Enhancement (M) (H) 111](#_Toc507670220)

[AC-17 (9) Control Enhancement (M) (H) 112](#_Toc507670221)

[AC-18 Wireless Access Restrictions (L) (M) (H) 114](#_Toc507670222)

[AC-18 (1) Control Enhancement (M) (H) 115](#_Toc507670223)

[AC-19 Access Control for Portable and Mobile Systems (L) (M) (H) 116](#_Toc507670224)

[AC-19 (5) Control Enhancement (M) (H) 117](#_Toc507670225)

[AC-20 Use of External Information Systems (L) (M) (H) 118](#_Toc507670226)

[AC-20 (1) Control Enhancement (M) (H) 120](#_Toc507670227)

[AC-20 (2) Control Enhancement (M) (H) 121](#_Toc507670228)

[AC-21 Information Sharing (M) (H) 122](#_Toc507670229)

[AC-22 Publicly Accessible Content (L) (M) (H) 124](#_Toc507670230)

[13.2. Awareness and Training (AT) 126](#_Toc507670231)

[AT-1 Security Awareness and Training Policy and Procedures (L) (M) 126](#_Toc507670232)

[AT-2 Security Awareness (L) (M) (H) 128](#_Toc507670233)

[AT-2 (2) Control Enhancement (M) (H) 131](#_Toc507670234)

[AT-3 Role-Based Security Training (L) (M) (H) 132](#_Toc507670235)

[AT-4 Security Training Records (L) (M) 133](#_Toc507670236)

[13.3. Audit and Accountability (AU) 135](#_Toc507670237)

[AU-1 Audit and Accountability Policy and Procedures (L) (M) 135](#_Toc507670238)

[AU-2 Audit Events (L) (M) (H) 137](#_Toc507670239)

[AU-2 (3) Control Enhancement (M) (H) 139](#_Toc507670240)

[AU-3 Content of Audit Records (L) (M) (H) 140](#_Toc507670241)

[AU-3 (1) Control Enhancement (M) 142](#_Toc507670242)

[AU-4 Audit Storage Capacity (L) (M) (H) 144](#_Toc507670243)

[AU-5 Response to Audit Processing Failures (L) (M) (H) 145](#_Toc507670244)

[AU-6 Audit Review, Analysis, and Reporting (L) (M) (H) 147](#_Toc507670245)

[AU-6 (1) Control Enhancement (M) (H) 149](#_Toc507670246)

[AU-6 (3) Control Enhancement (M) (H) 150](#_Toc507670247)

[AU-7 Audit Reduction and Report Generation (M) (H) 152](#_Toc507670248)

[AU-7 (1) Control Enhancement (M) (H) 153](#_Toc507670249)

[AU-8 Time Stamps (L) (M) (H) 155](#_Toc507670250)

[AU-8 (1) Control Enhancement (M) (H) 156](#_Toc507670251)

[AU-9 Protection of Audit Information (L) (M) (H) 161](#_Toc507670252)

[AU-9 (2) Control Enhancement (M) (H) 162](#_Toc507670253)

[AU-9 (4) Control Enhancement (M) (H) 163](#_Toc507670254)

[AU-11 Audit Record Retention (M) 164](#_Toc507670255)

[AU-12 Audit Generation (L) (M) (H) 166](#_Toc507670256)

[13.4. Security Assessment and Authorization (CA) 168](#_Toc507670257)

[CA-1 Certification, Authorization, Security Assessment Policy and Procedures (L) (M) 168](#_Toc507670258)

[CA-2 Security Assessments (L) (M) (H) 170](#_Toc507670259)

[CA-2 (1) Control Enhancement (L) (M) (H) 172](#_Toc507670260)

[CA-2 (2) Control Enhancement (M) (H) 173](#_Toc507670261)

[CA-2 (3) Control Enhancement (M) (H) 174](#_Toc507670262)

[CA-3 System Interconnections (L) (M) (H) 175](#_Toc507670263)

[CA-3 (3) Control Enhancement (M) (H) 179](#_Toc507670264)

[CA-3 (5) Control Enhancement (M) 180](#_Toc507670265)

[CA-5 Plan of Action and Milestones (L) (M) (H) 181](#_Toc507670266)

[CA-6 Security Authorization (L) (M) (H) 183](#_Toc507670267)

[CA-7 Continuous Monitoring (L) (M) (H) 184](#_Toc507670268)

[CA-7 (1) Control Enhancement (M) (H) 187](#_Toc507670269)

[CA-8 Penetration Testing (M) (H) 188](#_Toc507670270)

[CA-8 (1) Control Enhancement (M) (H) 190](#_Toc507670271)

[CA-9 Internal System Connections (L) (M) (H) 191](#_Toc507670272)

[13.5. Configuration Management (CM) 192](#_Toc507670273)

[CM-1 Configuration Management Policies and Procedures (L) (M) 192](#_Toc507670274)

[CM-2 Baseline Configuration (L) (M) (H) 194](#_Toc507670275)

[CM-2 (1) Control Enhancement (M) 195](#_Toc507670276)

[CM-2 (2) Control Enhancement (M) (H) 197](#_Toc507670277)

[CM-2 (3) Control Enhancement (M) 198](#_Toc507670278)

[CM-2 (7) Control Enhancement (M) (H) 199](#_Toc507670279)

[CM-3 Configuration Change Control (M) (H) 200](#_Toc507670280)

[CM-4 Security Impact Analysis (L) (M) (H) 203](#_Toc507670281)

[CM-5 Access Restrictions for Change (M) (H) 204](#_Toc507670282)

[CM-5 (1) Control Enhancement (M) (H) 205](#_Toc507670283)

[CM-5 (3) Control Enhancement (M) (H) 206](#_Toc507670284)

[CM-5 (5) Control Enhancement (M) (H) 207](#_Toc507670285)

[CM-6 Configuration Settings (L) (M) (H) 208](#_Toc507670286)

[CM-6 (1) Control Enhancement (M) (H) 211](#_Toc507670287)

[CM-7 Least Functionality (L) (M) (H) 212](#_Toc507670288)

[CM-7 (1) Control Enhancement (M) (H) 214](#_Toc507670289)

[CM-7 (2) Control Enhancement (M) (H) 215](#_Toc507670290)

[CM-7 (5) Control Enhancement (M) 216](#_Toc507670291)

[CM-8 Information System Component Inventory (L) (M) (H) 218](#_Toc507670292)

[CM-8 (1) Control Enhancement (M) (H) 220](#_Toc507670293)

[CM-8 (3) Control Enhancement (M) (H) 220](#_Toc507670294)

[CM-8 (5) Control Enhancement (M) (H) 222](#_Toc507670295)

[CM-9 Configuration Management Plan (M) (H) 223](#_Toc507670296)

[CM-10 Software Usage Restrictions (L) (M) (H) 224](#_Toc507670297)

[CM-10 (1) Control Enhancement (M) (H) 226](#_Toc507670298)

[CM-11 User-Installed Software (M) (H) 227](#_Toc507670299)

[13.6. Contingency Planning (CP) 229](#_Toc507670300)

[CP-1 Contingency Planning Policy and Procedures (L) (M) 229](#_Toc507670301)

[CP-2 Contingency Plan (L) (M) (H) 231](#_Toc507670302)

[CP-2 (1) Control Enhancement (M) (H) 235](#_Toc507670303)

[CP-2 (2) Control Enhancement (M) (H) 236](#_Toc507670304)

[CP-2 (3) Control Enhancement (M) (H) 236](#_Toc507670305)

[CP-2 (8) Control Enhancement (M) (H) 237](#_Toc507670306)

[CP-3 Contingency Training (L) (M) (H) 238](#_Toc507670307)

[CP-4 Contingency Plan Testing (H) 240](#_Toc507670308)

[CP-4 (1) Control Enhancement (M) (H) 241](#_Toc507670309)

[CP-6 Alternate Storage Site (M) (H) 242](#_Toc507670310)

[CP-6 (1) Control Enhancement (M) (H) 243](#_Toc507670311)

[CP-6 (3) Control Enhancement (M) (H) 244](#_Toc507670312)

[CP-7 Alternate Processing Site (M) (H) 245](#_Toc507670313)

[CP-7 (1) Control Enhancement (M) (H) 247](#_Toc507670314)

[CP-7 (2) Control Enhancement (M) (H) 248](#_Toc507670315)

[CP-7 (3) Control Enhancement (M) (H) 249](#_Toc507670316)

[CP-8 Telecommunications Services (M) (H) 250](#_Toc507670317)

[CP-8 (1) Control Enhancement (M) (H) 252](#_Toc507670318)

[CP-8 (2) Control Enhancement (M) (H) 253](#_Toc507670319)

[CP-9 Information System Backup (L) (M) (H) 254](#_Toc507670320)

[CP-9 (1) Control Enhancement (M) 258](#_Toc507670321)

[CP-9 (3) Control Enhancement (M) (H) 259](#_Toc507670322)

[CP-10 Information System Recovery and Reconstitution (L) (M) (H) 260](#_Toc507670323)

[CP-10 (2) Control Enhancement (M) (H) 262](#_Toc507670324)

[13.7. Identification and Authentication (IA) 263](#_Toc507670325)

[IA-1 Identification and Authentication Policy and Procedures (L) (M) 263](#_Toc507670326)

[IA-2 User Identification and Authentication (L) (M) (H) 265](#_Toc507670327)

[IA-2 (1) Control Enhancement (L) (M) (H) 266](#_Toc507670328)

[IA-2 (2) Control Enhancement (M) (H) 268](#_Toc507670329)

[IA-2 (3) Control Enhancement (M) (H) 270](#_Toc507670330)

[IA-2 (5) Control Enhancement (M) (H) 271](#_Toc507670331)

[IA-2 (8) Control Enhancement (M) (H) 272](#_Toc507670332)

[IA-2 (11) Control Enhancement (M) (H) 274](#_Toc507670333)

[IA-2 (12) Control Enhancement (L) (M) (H) 276](#_Toc507670334)

[IA-3 Device Identification and Authentication (M) (H) 277](#_Toc507670335)

[IA-4 Identifier Management (L) (M) 279](#_Toc507670336)

[IA-4 (4) Control Enhancement (M) (H) 282](#_Toc507670337)

[IA-5 Authenticator Management (L) (M) 283](#_Toc507670338)

[IA-5 (1) Control Enhancement (L) (M) 290](#_Toc507670339)

[IA-5 (2) Control Enhancement (M) (H) 295](#_Toc507670340)

[IA-5 (3) Control Enhancement (M) (H) 297](#_Toc507670341)

[IA-5 (4) Control Enhancement (M) 298](#_Toc507670342)

[IA-5 (6) Control Enhancement (M) (H) 300](#_Toc507670343)

[IA-5 (7) Control Enhancement (M) (H) 301](#_Toc507670344)

[IA-5 (11) Control Enhancement (L) (M) (H) 302](#_Toc507670345)

[IA-6 Authenticator Feedback (L) (M) (H) 303](#_Toc507670346)

[IA-7 Cryptographic Module Authentication (L) (M) (H) 304](#_Toc507670347)

[IA-8 Identification and Authentication (Non-Organizational Users) (L) (M) (H) 305](#_Toc507670348)

[IA-8 (1) Control Enhancement (L) (M) (H) 306](#_Toc507670349)

[IA-8 (2) Control Enhancement (L) (M) (H) 308](#_Toc507670350)

[IA-8 (3) Control Enhancement (L) (M) (H) 309](#_Toc507670351)

[IA-8 (4) Control Enhancement (L) (M) (H) 310](#_Toc507670352)

[13.8. Incident Response (IR) 311](#_Toc507670353)

[IR-1 Incident Response Policy and Procedures (L) (M) 311](#_Toc507670354)

[IR-2 Incident Response Training (L) (M) 313](#_Toc507670355)

[IR-3 Incident Response Testing (M) 314](#_Toc507670356)

[IR-3 (2) Control Enhancement (M) (H) 316](#_Toc507670357)

[IR-4 Incident Handling (L) (M) (H) 317](#_Toc507670358)

[IR-4 (1) Control Enhancement (M) (H) 318](#_Toc507670359)

[IR-5 Incident Monitoring (L) (M) (H) 319](#_Toc507670360)

[IR-6 Incident Reporting (L) (M) (H) 320](#_Toc507670361)

[IR-6 (1) Control Enhancement (M) (H) 322](#_Toc507670362)

[IR-7 Incident Response Assistance (L) (M) (H) 322](#_Toc507670363)

[IR-7 (1) Control Enhancement (M) (H) 323](#_Toc507670364)

[IR-7 (2) Control Enhancement (M) (H) 325](#_Toc507670365)

[IR-8 Incident Response Plan (L) (M) (H) 326](#_Toc507670366)

[IR-9 Information Spillage Response (M) (H) 330](#_Toc507670367)

[IR-9 (1) Control Enhancement (M) (H) 333](#_Toc507670368)

[IR-9 (2) Control Enhancement (M) 334](#_Toc507670369)

[IR-9 (3) Control Enhancement (M) (H) 335](#_Toc507670370)

[IR-9 (4) Control Enhancement (M) (H) 336](#_Toc507670371)

[13.9. Maintenance (MA) 337](#_Toc507670372)

[MA-1 System Maintenance Policy and Procedures (L) (M) 337](#_Toc507670373)

[MA-2 Controlled Maintenance (L) (M) (H) 340](#_Toc507670374)

[MA-3 Maintenance Tools (M) (H) 341](#_Toc507670375)

[MA-3 (1) Control Enhancement (M) (H) 342](#_Toc507670376)

[MA-3 (2) Control Enhancement (M) (H) 343](#_Toc507670377)

[MA-3 (3) Control Enhancement (M) (H) 344](#_Toc507670378)

[MA-4 Remote Maintenance (L) (M) (H) 345](#_Toc507670379)

[MA-4 (2) Control Enhancement (M) (H) 347](#_Toc507670380)

[MA-5 Maintenance Personnel (L) (M) (H) 348](#_Toc507670381)

[MA-5 (1) Control Enhancement (L) (M) 349](#_Toc507670382)

[MA-6 Timely Maintenance (M) (H) 350](#_Toc507670383)

[13.10. Media Protection (MP) 351](#_Toc507670384)

[MP-1 Media Protection Policy and Procedures (L) (M) 351](#_Toc507670385)

[MP-2 Media Access (L) (M) 353](#_Toc507670386)

[MP-3 Media Labeling (M) (H) 354](#_Toc507670387)

[MP-4 Media Storage (M) (H) 355](#_Toc507670388)

[MP-5 Media Transport (M) (H) 357](#_Toc507670389)

[MP-5 (4) Control Enhancement (M) (H) 358](#_Toc507670390)

[MP-6 Media Sanitization and Disposal (L) (M) 359](#_Toc507670391)

[MP-6 (2) Control Enhancement (M) 360](#_Toc507670392)

[MP-7 Media Use (L) (M) (H) 361](#_Toc507670393)

[MP-7 (1) Control Enhancement (M) (H) 362](#_Toc507670394)

[13.11. Physical and Environmental Protection (PE) 363](#_Toc507670395)

[PE-1 Physical and Environmental Protection Policy and Procedures (L) (M) 363](#_Toc507670396)

[PE-2 Physical Access Authorizations (L) (M) 366](#_Toc507670397)

[PE-3 Physical Access Control (L) (M) (H) 367](#_Toc507670398)

[PE-4 Access Control for Transmission Medium (M) (H) 369](#_Toc507670399)

[PE-5 Access Control for Output Devices (M) (H) 370](#_Toc507670400)

[PE-6 Monitoring Physical Access (L) (M) (H) 371](#_Toc507670401)

[PE-6 (1) Control Enhancement (M) (H) 372](#_Toc507670402)

[PE-8 Visitor Access Records (L) (M) (H) 373](#_Toc507670403)

[PE-9 Power Equipment and Cabling (M) (H) 374](#_Toc507670404)

[PE-10 Emergency Shutoff (M) (H) 375](#_Toc507670405)

[PE-11 Emergency Power (M) (H) 376](#_Toc507670406)

[PE-12 Emergency Lighting (L) (M) (H) 377](#_Toc507670407)

[PE-13 Fire Protection (L) (M) (H) 378](#_Toc507670408)

[PE-13 (2) Control Enhancement (M) (H) 379](#_Toc507670409)

[PE-13 (3) Control Enhancement (M) (H) 380](#_Toc507670410)

[PE-14 Temperature and Humidity Controls (L) (M) (H) 381](#_Toc507670411)

[PE-14 (2) Control Enhancement (M) (H) 382](#_Toc507670412)

[PE-15 Water Damage Protection (L) (M) (H) 383](#_Toc507670413)

[PE-16 Delivery and Removal (L) (M) (H) 383](#_Toc507670414)

[PE-17 Alternate Work Site (M) (H) 384](#_Toc507670415)

[13.12. Planning (PL) 386](#_Toc507670416)

[PL-1 Security Planning Policy and Procedures (L) (M) 386](#_Toc507670417)

[PL-2 System Security Plan (L) (M) (H) 388](#_Toc507670418)

[PL-2 (3) Control Enhancement (M) (H) 390](#_Toc507670419)

[PL-4 Rules of Behavior (L) (M) 391](#_Toc507670420)

[PL-4 (1) Control Enhancement (M) (H) 393](#_Toc507670421)

[PL-8 Information Security Architecture (M) (H) 394](#_Toc507670422)

[13.13. Personnel Security (PS) 396](#_Toc507670423)

[PS-1 Personnel Security Policy and Procedures (L) (M) 396](#_Toc507670424)

[PS-2 Position Categorization (L) (M) 398](#_Toc507670425)

[PS-3 Personnel Screening (L) (M) (H) 400](#_Toc507670426)

[PS-3 (3) Control Enhancement (M) (H) 402](#_Toc507670427)

[PS-4 Personnel Termination (L) (M) 404](#_Toc507670428)

[PS-5 Personnel Transfer (L) (M) 407](#_Toc507670429)

[PS-6 Access Agreements (L) (M) 410](#_Toc507670430)

[PS-7 Third-Party Personnel Security (L) (M) 413](#_Toc507670431)

[PS-8 Personnel Sanctions (L) (M) 415](#_Toc507670432)

[13.14. Risk Assessment (RA) 417](#_Toc507670433)

[RA-1 Risk Assessment Policy and Procedures (L) (M) 417](#_Toc507670434)

[RA-2 Security Categorization (L) (M) (H) 419](#_Toc507670435)

[RA-3 Risk Assessment (L) (M) 421](#_Toc507670436)

[RA-5 Vulnerability Scanning (L) (M) (H) 424](#_Toc507670437)

[RA-5 (1) Control Enhancement (M) (H) 427](#_Toc507670438)

[RA-5 (2) Control Enhancement (M) (H) 428](#_Toc507670439)

[RA-5 (3) Control Enhancement (M) (H) 429](#_Toc507670440)

[RA-5 (5) Control Enhancement (M) (H) 430](#_Toc507670441)

[RA-5 (6) Control Enhancement (M) (H) 431](#_Toc507670442)

[RA-5 (8) Control Enhancement (L) (M) (H) 432](#_Toc507670443)

[13.15. System and Services Acquisition (SA) 433](#_Toc507670444)

[SA-1 System and Services Acquisition Policy and Procedures (L) (M) 433](#_Toc507670445)

[SA-2 Allocation of Resources (L) (M) (H) 435](#_Toc507670446)

[SA-3 System Development Life Cycle (L) (M) (H) 436](#_Toc507670447)

[SA-4 Acquisitions Process (L) (M) (H) 439](#_Toc507670448)

[SA-4 (1) Control Enhancement (M) (H) 444](#_Toc507670449)

[SA-4 (2) Control Enhancement (L) (M) 445](#_Toc507670450)

[SA-4 (8) Control Enhancement (M) (H) 446](#_Toc507670451)

[SA-4 (9) Control Enhancement (M) (H) 447](#_Toc507670452)

[SA-4 (10) Control Enhancement (M) (H) 448](#_Toc507670453)

[SA-5 Information System Documentation (L) (M) 449](#_Toc507670454)

[SA-8 Security Engineering Principles (M) (H) 453](#_Toc507670455)

[SA-9 External Information System Services (L) (M) (H) 454](#_Toc507670456)

[SA-9 (1) Control Enhancement (M) (H) 456](#_Toc507670457)

[SA-9 (2) Control Enhancement (M) (H) 458](#_Toc507670458)

[SA-9 (4) Control Enhancement (M) (H) 459](#_Toc507670459)

[SA-9 (5) Control Enhancement (M) (H) 460](#_Toc507670460)

[SA-10 Developer Configuration Management (M) (H) 461](#_Toc507670461)

[SA-10 (1) Control Enhancement (M) (H) 463](#_Toc507670462)

[SA-11 Developer Security Testing and Evaluation (M) (H) 464](#_Toc507670463)

[SA-11 (1) Control Enhancement (M) (H) 466](#_Toc507670464)

[SA-11 (2) Control Enhancement (M) (H) 467](#_Toc507670465)

[SA-11 (8) Control Enhancement (M) (H) 468](#_Toc507670466)

[13.16. System and Communications Protection (SC) 469](#_Toc507670467)

[SC-1 System and Communications Protection Policy and Procedures (L) (M) 469](#_Toc507670468)

[SC-2 Application Partitioning (M) (H) 471](#_Toc507670469)

[SC-4 Information in Shared Resources (M) (H) 472](#_Toc507670470)

[SC-5 Denial of Service Protection (L) (M) (H) 474](#_Toc507670471)

[SC-6 Resource Availability (M) (H) 475](#_Toc507670472)

[SC-7 Boundary Protection (L) (M) (H) 476](#_Toc507670473)

[SC-7 (3) Control Enhancement (M) (H) 478](#_Toc507670474)

[SC-7 (4) Control Enhancement (M) 478](#_Toc507670475)

[SC-7 (5) Control Enhancement (M) (H) 480](#_Toc507670476)

[SC-7 (7) Control Enhancement (M) (H) 481](#_Toc507670477)

[SC-7 (8) Control Enhancement (M) (H) 482](#_Toc507670478)

[SC-7 (12) Control Enhancement (M) 483](#_Toc507670479)

[SC-7 (13) Control Enhancement (M) 484](#_Toc507670480)

[SC-7 (18) Control Enhancement (M) (H) 485](#_Toc507670481)

[SC-8 Transmission confidentiality and Integrity (M) (H) 486](#_Toc507670482)

[SC-8 (1) Control Enhancement (M) (H) 488](#_Toc507670483)

[SC-10 Network Disconnect (M) 489](#_Toc507670484)

[SC-12 Cryptographic Key Establishment & Management (L) (M) (H) 490](#_Toc507670485)

[SC-12 (2) Control Enhancement (M) (H) 491](#_Toc507670486)

[SC-12 (3) Control Enhancement (M) (H) 493](#_Toc507670487)

[SC-13 Use of Cryptography (L) (M) (H) 494](#_Toc507670488)

[SC-15 Collaborative Computing Devices (M) (H) 496](#_Toc507670489)

[SC-17 Public Key Infrastructure Certificates (M) (H) 498](#_Toc507670490)

[SC-18 Mobile Code (M) (H) 499](#_Toc507670491)

[SC-19 Voice Over Internet Protocol (M) (H) 501](#_Toc507670492)

[SC-20 Secure Name / Address Resolution Service (Authoritative Source) (L) (M) (H) 503](#_Toc507670493)

[SC-21 Secure Name / Address Resolution Service (Recursive or Caching Resolver) (L) (M) (H) 504](#_Toc507670494)

[SC-22 Architecture and Provisioning for Name / Address Resolution Service (L) (M) (H) 505](#_Toc507670495)

[SC-23 Session Authenticity (M) (H) 506](#_Toc507670496)

[SC-28 Protection of Information at Rest (M) (H) 507](#_Toc507670497)

[SC-28 (1) Control Enhancement (M) 509](#_Toc507670498)

[SC-39 Process Isolation (L) (M) (H) 510](#_Toc507670499)

[13.17. System and Information Integrity (SI) 511](#_Toc507670500)

[SI-1 System and Information Integrity Policy and Procedures (L) (M) 511](#_Toc507670501)

[SI-2 Flaw Remediation (L) (M) (H) 513](#_Toc507670502)

[SI-2 (2) Control Enhancement (M) (H) 515](#_Toc507670503)

[SI-2 (3) Control Enhancement (M) (H) 516](#_Toc507670504)

[SI-3 Malicious Code Protection (L) (M) 518](#_Toc507670505)

[SI-3 (1) Control Enhancement (M) (H) 520](#_Toc507670506)

[SI-3 (2) Control Enhancement (M) (H) 521](#_Toc507670507)

[SI-3 (7) Control Enhancement (M) (H) 522](#_Toc507670508)

[SI-4 Information System Monitoring (L) (M) (H) 523](#_Toc507670509)

[SI-4 (1) Control Enhancement (M) (H) 526](#_Toc507670510)

[SI-4 (2) Control Enhancement (M) (H) 527](#_Toc507670511)

[SI-4 (4) Control Enhancement (M) (H) 528](#_Toc507670512)

[SI-4 (5) Control Enhancement (M) (H) 529](#_Toc507670513)

[SI-4 (14) Control Enhancement (M) (H) 530](#_Toc507670514)

[SI-4 (16) Control Enhancement (M) (H) 531](#_Toc507670515)

[SI-4 (23) Control Enhancement (M) (H) 532](#_Toc507670516)

[SI-5 Security Alerts & Advisories (L) (M) (H) 533](#_Toc507670517)

[SI-6 Security Functionality Verification (M) (H) 535](#_Toc507670518)

[SI-7 Software & Information Integrity (M) (H) 537](#_Toc507670519)

[SI-7 (1) Control Enhancement (M) (H) 539](#_Toc507670520)

[SI-7 (7) Control Enhancement (M) (H) 541](#_Toc507670521)

[SI-8 Spam Protection (M) (H) 542](#_Toc507670522)

[SI-8 (1) Control Enhancement (M) (H) 543](#_Toc507670523)

[SI-8 (2) Control Enhancement (M) (H) 544](#_Toc507670524)

[SI-10 Information Input Validation (M) (H) 545](#_Toc507670525)

[SI-11 Error Handling (M) (H) 546](#_Toc507670526)

[SI-12 Information Output Handling and Retention (L) (M) (H) 547](#_Toc507670527)

[SI-16 Memory Protection (M) (H) 548](#_Toc507670528)

[14. Acronyms 550](#_Toc507670529)

[15. Attachments 551](#_Toc507670530)

[ATTACHMENT 1 - Information Security Policies and Procedures 552](#_Toc507670531)

[ATTACHMENT 2 - User Guide 553](#_Toc507670532)

[ATTACHMENT 3 – e-Authentication Worksheet 554](#_Toc507670533)

[Introduction and Purpose 554](#_Toc507670534)

[Information System Name/Title 554](#_Toc507670535)

[E-Authentication Level Definitions 554](#_Toc507670536)

[Review Maximum Potential Impact Levels 555](#_Toc507670537)

[E-Authentication Level Selection 555](#_Toc507670538)

[ATTACHMENT 4 – PTA / PIA 556](#_Toc507670539)

[Privacy Overview and Point of Contact (POC) 556](#_Toc507670540)

[Applicable Laws and Regulations 556](#_Toc507670541)

[Applicable Standards and Guidance 557](#_Toc507670542)

[Personally Identifiable Information (PII) 557](#_Toc507670543)

[Privacy Threshold Analysis 557](#_Toc507670544)

[Qualifying Questions 558](#_Toc507670545)

[Designation 558](#_Toc507670546)

[ATTACHMENT 5 - Rules of Behavior 559](#_Toc507670547)

[ATTACHMENT 6 – Information System Contingency Plan 560](#_Toc507670548)

[ATTACHMENT 7 - Configuration Management Plan 561](#_Toc507670549)

[ATTACHMENT 8 - Incident Response Plan 562](#_Toc507670550)

[ATTACHMENT 9 - CIS Report and Worksheet 563](#_Toc507670551)

[ATTACHMENT 10 - FIPS 199 564](#_Toc507670552)

[Introduction and Purpose 564](#_Toc507670553)

[Scope 564](#_Toc507670554)

[System Description 564](#_Toc507670555)

[Methodology 565](#_Toc507670556)

[ATTACHMENT 11 - Separation of Duties Matrix 569](#_Toc507670557)

[ATTACHMENT 12 – FedRAMP Laws and Regulations 570](#_Toc507670558)

[ATTACHMENT 13 – FedRAMP Inventory Workbook 571](#_Toc507670559)

[ATTACHMENT 14 – Ports, Protocols and Services 572](#_Toc507670560)

[ATTACHMENT 15 – Office 365 Internal Documents 573](#_Toc507670561)

List of Tables

[Table 1‑1 Information System Name and Title 1](#_Toc507666052)

[Table 2‑1 Security Categorization 1](#_Toc507666053)

[Table 2‑2 Sensitivity Categorization of Information Types 3](#_Toc507666054)

[Table 2‑3 Security Impact Level 3](#_Toc507666055)

[Table 2‑4 Baseline Security Configuration 3](#_Toc507666056)

[Table 3‑1 Information System Owner 4](#_Toc507666057)

[Table 5‑1 Information System Management Point of Contact 5](#_Toc507666058)

[Table 5‑2 Information System Technical Point of Contact 5](#_Toc507666059)

[Table 6‑1 CSP Name Internal ISSO (or Equivalent) Point of Contact 5](#_Toc507666060)

[Table 6‑2 AO ISSO Point of Contact 6](#_Toc507666061)

[Table 7‑1 System Status 6](#_Toc507666062)

[Table 8‑1 Service Layers Represented in this SSP 7](#_Toc507666063)

[Table 8‑2 Cloud Deployment Model Represented in this SSP 7](#_Toc507666064)

[Table 8‑3 Leveraged Authorizations 8](#_Toc507666065)

[Table 9‑1 Personnel Roles and Privileges 14](#_Toc507666066)

[Table 11‑1 System Interconnections 36](#_Toc507666067)

[Table 12‑1 Office 365 MultiTenant Cloud Laws and Regulations 37](#_Toc507666068)

[Table 12‑2 Office 365 MultiTenant Cloud Standards and Guidance 37](#_Toc507666069)

[Table 13‑1 Summary of Required Security Controls 38](#_Toc507666070)

[Table 13‑2 Control Origination and Definitions 46](#_Toc507666071)

[Table 13‑3 CA-3 Authorized Connections 176](#_Toc507666072)

[Table 15‑1 Attachment File Naming Convention 551](#_Toc507666073)

[Table 15‑2 Information System Name and Title 554](#_Toc507666074)

[Table 15‑3 Potential Impacts for Assurance Levels 555](#_Toc507666075)

[Table 15‑4 E-Authentication Level 555](#_Toc507666076)

[Table 15‑5 - Information System Name; Privacy POC 556](#_Toc507666077)

[Table 15‑6 Office 365 MultiTenant Cloud Laws and Regulations 556](#_Toc507666078)

[Table 15‑7 Office 365 MultiTenant Cloud Standards and Guidance 557](#_Toc507666079)

[Table 15‑8 CSP Applicable Information Types with Security Impact Levels Using NIST SP 800-60 V2 R1 566](#_Toc507666080)

[Table 15‑9 FedRAMP Templates that Reference FedRAMP Laws and Regulations Standards and Guidance 570](#_Toc507666081)

[Table 15‑10 Office 365 Internal Documents 573](#_Toc507666082)

List of Figures

[Figure 9‑1 Office 365 MT and Office 365 GCC Separation Diagram 11](#_Toc507665830)

[Figure 9‑2 Network Diagram 16](#_Toc507665831)

[Figure 9‑3 Exchange Online Data Flows 17](#_Toc507665832)

[Figure 9‑4 SharePoint Online Data Flows 18](#_Toc507665833)

[Figure 9‑5 Skype for Business Data Flows 20](#_Toc507665834)

[Figure 9‑6 Information Protection Data Flows 22](#_Toc507665835)

[Figure 9‑7 Office Online Data Flows 23](#_Toc507665836)

[Figure 9‑8 Security Workload Environment Data Flows 24](#_Toc507665837)

[Figure 9‑9 DNS Data Flows 25](#_Toc507665838)

[Figure 9‑10 Suite User Experience Data Flows 26](#_Toc507665839)

[Figure 9‑11 Office Service Data Flows 27](#_Toc507665840)

[Figure 9‑12 Azure Active Directory Data Flows 29](#_Toc507665841)

[Figure 9‑13 Microsoft Teams Data Flows 30](#_Toc507665842)

[Figure 9‑14 Bing Data Flows 31](#_Toc507665843)

[Figure 9‑15 Outlook Mobile Data Flows 32](#_Toc507665844)

[Figure 9‑16 Delve Data Flows 33](#_Toc507665845)

[Figure 10‑1 Data Flow Diagram 35](#_Toc507665846)

System Security Plan Approvals

Cloud Service Provider Signatures

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | | | |
| Name | Greg Roberts | | Date |  |
| Title | Authorizing Official Microsoft | | | |
| Cloud Service Provider | | Microsoft | | |
|  | | | | |
|  | | | | |
|  | | | | |
| Name | Shawn Veney | | Date |  |
| Title | Information System Security Officer | | | |
| Cloud Service Provider | | Microsoft | | |
|  | | | | |

1. Information System Name/Title

This System Security Plan provides an overview of the security requirements for the Office 365 MultiTenant ( Office 365 MT) and describes the controls in place or planned for implementation to provide a level of security appropriate for the information to be transmitted, processed or stored by the system. Information security is vital to our critical infrastructure and its effective performance and protection is a key component of our national security program. Proper management of information technology systems is essential to ensure the confidentiality, integrity and availability of the data transmitted, processed or stored by the Office 365 MT information system.

The security safeguards implemented for the Office 365 MT system meet the policy and control requirements set forth in this System Security Plan. All systems are subject to monitoring consistent with applicable laws, regulations, agency policies, procedures and practices.

Table 1‑1 Information System Name and Title

| Unique Identifier | Information System Name | Information System Abbreviation |
| --- | --- | --- |
| F1209231600 | Office 365 MultiTenant | Office 365 MT |

1. Information System Categorization

The overall information system sensitivity categorization is recorded in Table 2‑1 Security Categorization that follows. Directions for attaching the FIPS 199 document may be found in the following section: ATTACHMENT 10 - FIPS 199.

Table 2‑1 Security Categorization

|  |  |
| --- | --- |
| System Sensitivity Level: | Moderate (M) |

* 1. Information Types

This section describes how the information types used by the information system are categorized for confidentiality, integrity and availability sensitivity levels.

The following tables identify the information types that are input, stored, processed and/or output from Office 365 MT. The selection of the information types is based on guidance provided by the Office of Management and Budget (OMB) Federal Enterprise Architecture Program Management Office Business Reference Model 2.0 and FIPS Pub 199, Standards for Security Categorization of Federal Information and Information Systems which is based on NIST Special Publication (SP) 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories.

The tables also identify the security impact levels for confidentiality, integrity and availability for each of the information types expressed as low, moderate, or high. The security impact levels are based on the potential impact definitions for each of the security objectives (i.e., confidentiality, integrity and availability) discussed in NIST SP 800-60 and FIPS Pub 199.

The potential impact is low if—

* The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
* A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

The potential impact is moderate if—

* The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
* A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

The potential impact is high if—

* The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
* A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

Table 2‑2 Sensitivity Categorization of Information Types

| Information Type  (Use only information types from NIST SP 800-60, Volumes I and II as amended) | NIST 800-60 identifier for Associated Information Type | Confidentiality | Integrity | Availability |
| --- | --- | --- | --- | --- |
| System Maintenance | C.3.5.3 | Low (L) | Moderate (M) | Low (L) |
| IT Infrastructure Maintenance | C.3.5.4 | Low (L) | Low (L) | Low (L) |
| Information System Security | C.3.5.5 | Low (L) | Moderate (M) | Moderate (M) |
| Record Retention | C.3.5.6 | Low (L) | Low (L) | Low (L) |
| Information Management | C.3.5.7 | Low (L) | Moderate (M) | Low (L) |
| System and Network Monitoring | C.3.5.8 | Moderate (M) | Moderate (M) | Low (L) |
| Official Information Dissemination | C.2.6.2 | Low (L) | Low (L) | Moderate (M) |
| Lifecycle/Change Management | C.3.5.2 | Low (L) | Moderate (M) | Low (L) |

* 1. Security Objectives Categorization (FIPS 199)

Based on the information provided in Table 2‑2 Sensitivity Categorization of Information Types, for the Office 365 MT, default to the high-water mark for the Information Types as identified in Table 2‑3 Security Impact Level below.

Table 2‑3 Security Impact Level

| Security Objective | Low, Moderate or High |
| --- | --- |
| Confidentiality | Moderate (M) |
| Integrity | Moderate (M) |
| Availability | Moderate (M) |

Through review and analysis, it has been determined that the baseline security categorization for the Office 365 MT system is listed in the Table 2‑4 Baseline Security Configuration that follows.

Table 2‑4 Baseline Security Configuration

|  |  |
| --- | --- |
| Office 365 MT Security Categorization | Moderate (M) |

Using this categorization, in conjunction with the risk assessment and any unique security requirements, we have established the security controls for this system, as detailed in this SSP.

* 1. E-Authentication Determination

The e-Authentication information may be found in section: Section 15 Attachments E-Authentication Level Selection.

Note: Refer to OMB Memo M-04-04 E-Authentication Guidance for Federal Agencies for more information on e-Authentication.

The e-authentication level is Level 3: High confidence in the asserted identity’s validity

Additional e-Authentication information can be found in Section 15 Attachments E-Authentication Level Selection.

1. Information System Owner

The following individual is identified as the system owner or functional proponent/advocate for this system.

Table 3‑1 Information System Owner

| Information System Owner Information | |
| --- | --- |
| Name | Greg Roberts |
| Title | Microsoft Office 365 Principal Group Program Manager |
| Company / Organization | Microsoft / Office 365 |
| Address | 1 Microsoft Way, Redmond, WA 98052 |
| Phone Number | +1 (425) 722-6538 |
| Email Address | groberts@microsoft.com |

1. Authorizing Official

The Authorizing Official (AO) or Designated Approving Authority (DAA) for this information system is the Federal Risk Authorization Management Program (FedRAMP), Joint Authorization Board (JAB) as comprised of member representatives from the General Services Administration (GSA), Department of Defense (DoD) and Department of Homeland Security (DHS).

1. Other Designated Contacts

The following individual(s) identified below possess in-depth knowledge of this system and/or its functions and operation.

Table 5‑1 Information System Management Point of Contact

| Information System Management Point of Contact | |
| --- | --- |
| Name | Brian Smith |
| Title | Sr. Program Manager |
| Company / Organization | Microsoft / Office 365 |
| Address | 1 Microsoft Way, Redmond, WA 98052 |
| Phone Number | (425) 722-8160 |
| Email Address | smith.brian@microsoft.com |

Table 5‑2 Information System Technical Point of Contact

| Information System Technical Point of Contact | |
| --- | --- |
| Name | Shawn Veney |
| Title | Office 365 Principal Architect |
| Company / Organization | Microsoft/ Office 365 Foundation |
| Address | 1 Microsoft Way, Redmond, WA 98052 |
| Phone Number | +1 (425) 706-9386 |
| Email Address | shawnven@microsoft.com |

1. Assignment of Security Responsibility

The Information System Security Officers (ISSO), or their equivalent, identified below, have been appointed in writing and are deemed to have significant cyber and operational role responsibilities.

Table 6‑1 CSP Name Internal ISSO (or Equivalent) Point of Contact

| CSP Name Internal ISSO (or Equivalent) Point of Contact | |
| --- | --- |
| Name | Shawn Veney |
| Title | Office 365 Principal Architect |
| Company / Organization | Microsoft/ Office 365 Foundation |
| Address | 1 Microsoft Way, Redmond, WA 98052 |
| Phone Number | +1 (425) 70706-9386 |
| Email Address | shawnven@microsoft.com |

Table 6‑2 AO ISSO Point of Contact

|  |  |
| --- | --- |
| AO ISSO Point of Contact | |
| Name |  |
| Title |  |
| Organization |  |
| Address |  |
| Phone Number |  |
| Email Address |  |

1. Information System Operational Status

The system is currently in the life-cycle phase shown in Table 7‑1 System Status that follows. (Only operational systems can be granted an ATO).

Table 7‑1 System Status

| System Status | | |
| --- | --- | --- |
| ☒ | Operational | The system is operating and in production. |
| ☐ | Under Development | The system is being designed, developed, or implemented |
| ☐ | Major Modification | The system is undergoing a major change, development, or transition. |
| ☐ | Other | Explain: |

1. Information System Type

The Office 365 MT makes use of unique managed service provider architecture layer(s).

* 1. Cloud Service Models

Information systems, particularly those based on cloud architecture models, are made up of different service layers. Below are some questions that help the system owner determine if their system is a cloud followed by specific questions to help the system owner determine the type of cloud.

|  |  |
| --- | --- |
| Question (Yes/No) | Conclusion |
| Does the system use virtual machines? | A no response means that system is most likely not a cloud. |
| Does the system have the ability to expand its capacity to meet customer demand? | A no response means that the system is most likely not a cloud. |
| Does the system allow the consumer to build anything other than servers? | A no response means that the system is an IaaS. A yes response means that the system is either a PaaS or a SaaS. |
| Does the system offer the ability to create databases? | A yes response means that the system is a PaaS. |
| Does the system offer various developer toolkits and APIs? | A yes response means that the system is a PaaS. |
| Does the system offer only applications that are available by obtaining a login? | A yes response means that system is a SaaS. A no response means that the system is either a PaaS or an IaaS. |

The layers of the Office 365 MT defined in this SSP are indicated in Table 8‑1 Service Layers Represented in this SSP that follows.

Table 8‑1 Service Layers Represented in this SSP

| Service Provider Architecture Layers | | |
| --- | --- | --- |
| ☒ | Software as a Service (SaaS) | Major Application |
| ☐ | Platform as a Service (PaaS) | Major Application |
| ☐ | Infrastructure as a Service (IaaS) | General Support System |
| ☐ | Other | Explain: |

Note: Refer to NIST SP 800-145 for information on cloud computing architecture models.

* 1. Cloud Deployment Models

Information systems are made up of different deployment models. The deployment models of the Office 365 MT that are defined in this SSP and are not leveraged by any other FedRAMP Authorizations, are indicated in Table 8‑2 Cloud Deployment Model Represented in this SSP that follows.

Table 8‑2 Cloud Deployment Model Represented in this SSP

| Service Provider Cloud Deployment Model | | |
| --- | --- | --- |
| ☒ | Public | Cloud services and infrastructure supporting multiple organizations and agency clients |
| ☐ | Private | Cloud services and infrastructure dedicated to a specific organization/agency and no other clients |
| ☐ | Government Only Community | Cloud services and infrastructure shared by several organizations/agencies with same policy and compliance considerations |
| ☐ | Hybrid | Explain: (e.g., cloud services and infrastructure that provides private cloud for secured applications and data where required and public cloud for other applications and data) |

* 1. Leveraged Authorizations

The Office 365 MT plans to leverage a pre-existing FedRAMP Authorization. FedRAMP Authorizations leveraged by Office 365 MT are listed in Table 8‑3 Leveraged Authorizations that follows.

Table 8‑3 Leveraged Authorizations

| Leveraged Information System Name | Leveraged Service Provider Owner | Date Granted |
| --- | --- | --- |
| Microsoft Azure Commercial Cloud Solution (F1209051525) | Microsoft | 9/25/2017 |
| Akamai Content Delivery Services (Akamai CDN) (F1206061353) | Akamai | 8/26/2013 |

1. General System Description

This section includes a general description of Office 365 Multi-Tenant.

* 1. System Function or Purpose

This service overview focuses on providing the background necessary to understand the implementation details in section 13 of this SSP. First, there will be a brief discussion of the customer-facing features and functionality of Office 365 MT. Next, there will be a high-level overview of the security architecture of Office 365 MT. Third, there will be a summary for each component of Office 365 MT explaining how that component fits within the Office 365 MT security architecture.

* + 1. Service Summary

Office 365 MT is a multi-tenant cloud computing-based subscription service offering from Microsoft. Cloud computing has been defined by NIST as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or cloud provider interaction. Further, as defined within NIST SP 800-145 (The NIST Definition of Cloud Computing), the service model for Office 365 MT is Software-as-a-Service (SaaS). SaaS is a model of software deployment whereby one or more applications and the computational resources to run them are provided for use on demand as a turnkey service. Its main purpose is to reduce the total cost of hardware and software development, maintenance, and operations. Security provisions are carried out mainly by the cloud provider. The cloud subscriber does not manage or control the underlying cloud infrastructure or individual applications, except for preference selections and limited administrative application settings.

Office 365 MT provides customers with cloud versions of Exchange Online (EXO), SharePoint Online (SPO) (including Access Online, Project Online, and OneDrive for Business), Skype for Business (SFB), Information Protection (IP), Office Online (WAC), Security Workload Environment (SWE), Domain Name Service (DNS), Office 365 Suite User Experience (SUE), Office Service Infrastructure (OSI), Microsoft Teams (MSTeams), Bing, Outlook Mobile (OLM), and Delve. Detailed service descriptions for each service team are included in section 9.5 of this SSP.

Office 365 MT has a number of supporting services in addition to these core, customer-facing services. Each core and supporting service is supported by a unique group of developers, testers, and administrators referred to throughout this document as a “service team”. Each service is deployed onto service-specific servers, whether physical or virtual. While each service team follows Office 365 policy, their services may have unique implementations of some security controls. For this reason, the SSP provides unique answers for each service where necessary. Where services have identical implementations, the implementation details are combined. A description of each service, including an explanation of that service team’s high-level security architecture is provided in section 9.1.3 of this SSP.

* + 1. Security Overview

Office 365 MT security and compliance is managed by a team named “Office 365 Trust”. Office 365 Trust ensures that all services comply with security controls, manages audits, writes and enforces Microsoft policy, manages POA&Ms, and manages FedRAMP continuous monitoring. Please see the applicable controls from section 13 of this SSP for details on implementations of these responsibilities. Incident Response is managed for all service teams by “Office 365 Security Incident Response”; details can be found in the Incident Response controls in section 13 of this SSP. Contingency and continuity planning are managed by the “Business Continuity Management Team” (BCM) in coordination with Office 365 Trust; details can be found in the Contingency Planning controls in section 13 of this SSP.

All Office 365 MT services are hosted on Azure IaaS/PaaS, which has a FedRAMP P-ATO. In this case, the physical servers are owned by Office 365 MT, the operating system and software are managed by Office 365 MT, and network layer and network layer protections are implemented by Azure. The configuration of the network layer/protection is managed by Office 365 MT in coordination with Azure. Azure is responsible for physical and environmental security. These servers are located in Azure continental United States (CONUS) data centers as described in the Azure SSP. Details of Office 365 MT service teams are hosted on Azure are located in section 9.5 of this SSP.

Implementation of network layer security controls between the public internet and Office 365 MT is inherited from Azure. In all cases, there is a default deny-all policy for inbound traffic; only the specific ports and protocols required for the operation of the service and listed in section Attachment 14 - Ports, Protocols and Services of this SSP are allowed. All traffic leaving the Office 365 MT boundary is encrypted and restricted as discussed primarily in the System and Communications Protection control family of this SSP. Section 9.2 has a detailed discussion of data flows crossing the Office 365 MT accreditation boundary.

Office 365 MT was built from the ground up as a public, multitenant cloud solution; taking into account the benefits and risks associated with that architecture. Microsoft designed Office 365 MT with the assumption that tenants of the system may be hostile and built in protections to ensure that tenants of Office 365 MT do not pose a risk to each other. Office 365 MT offers customers the scalability and cost savings of a multitenant cloud while preventing a weak security implementation from impacting the security of Office 365 MT or another Office 365 MT tenant.

Office 365 MT was designed using the principles of defense in depth. Cross-tenant protections are implemented at the application layer to ensure that customers cannot compromise Office 365 MT applications to gain unauthorized access to the information of other tenants. Protections are also implemented at the network layer to prevent interception of network traffic and resource starvation attacks. Protections are additionally implemented at the operating system layer to prevent side channel attacks. Details regarding the protections implemented to prevent cross-tenant attacks are documented in “Microsoft Office 365 Tenant Separation”.

* + 1. Active Directory Federation Service (ADFS)

Microsoft requires that government customers of Office 365 MT use Active Directory Federation Services (ADFS) for user provisioning, identity management, authentication, and permissions management. ADFS allows customers to maintain control of user identification and authentication from within their network and operating environment when using Office 365 MT.

The implementation of ADFS creates a one-way trust from Office 365 MT to the customer’s existing AD infrastructure. When a Federal user attempts to access Office 365 MT, the user is redirected to a login page that is hosted on the customer’s ADFS server. The user provides their credentials to this ADFS server, which validates them using the customer’s existing Active Directory infrastructure. If the credentials are validated, the customer’s ADFS server issues a SAML ticket containing information about the user’s identity and group membership. The customer ADFS server signs this ticket using one half of an asymmetric key pair and the user sends the ticket to Office 365 MT via encrypted TLS. Office 365 MT validates the signature using the other half of the asymmetric key pair and grants access based on the ticket.

The use of ADFS requires directory synchronization between Office 365 MT and the customer’s ADFS server for user provisioning and de-provisioning. This synchronization occurs over a mutually authenticated encrypted TLS connection. Additional information about the process of deploying ADFS and directory synchronization can be found at:http://technet.microsoft.com/en-us/library/jj205462.aspx

Use of ADFS is required for FedRAMP-compliant use of Office 365 MT; for details of how non-government customers who do not use ADFS authenticate, please see section 9.5.11 of this SSP. Use of ADFS means that the customer retains full or partial responsibility for many security controls, particularly within the Access Control and Identification and Authentication control families. Information about how the ADFS requirement affects specific security controls is provided with the relevant controls in section 13 of this SSP.

* + 1. Office 365 MT vs Office 365 GCC

Microsoft is aware that some Federal customers have additional security requirements beyond those specified by FedRAMP. One frequent requirement is that Microsoft administrators with logical access to customer content are U.S. citizens and undergo additional background screening[[1]](#footnote-2). To meet this requirement, Microsoft offers an enhanced version of the Office 365 MT product which is marketed as “Office 365 Government Community Cloud” (Office 365 GCC). Microsoft administrators with logical access to customer content stored or cached in Office 365 Exchange, Skype for Business, Information Protection, SharePoint Online, Office Web Applications, Security Workload Environment, Suite User Experience, Office Service Infrastructure, Bing, and Microsoft Teams are subject to these additional citizenship requirements and background screening. As a measure to further isolate services that store customer content, these service teams are deployed to servers dedicated to U.S. Federal, State, and Local government customers.

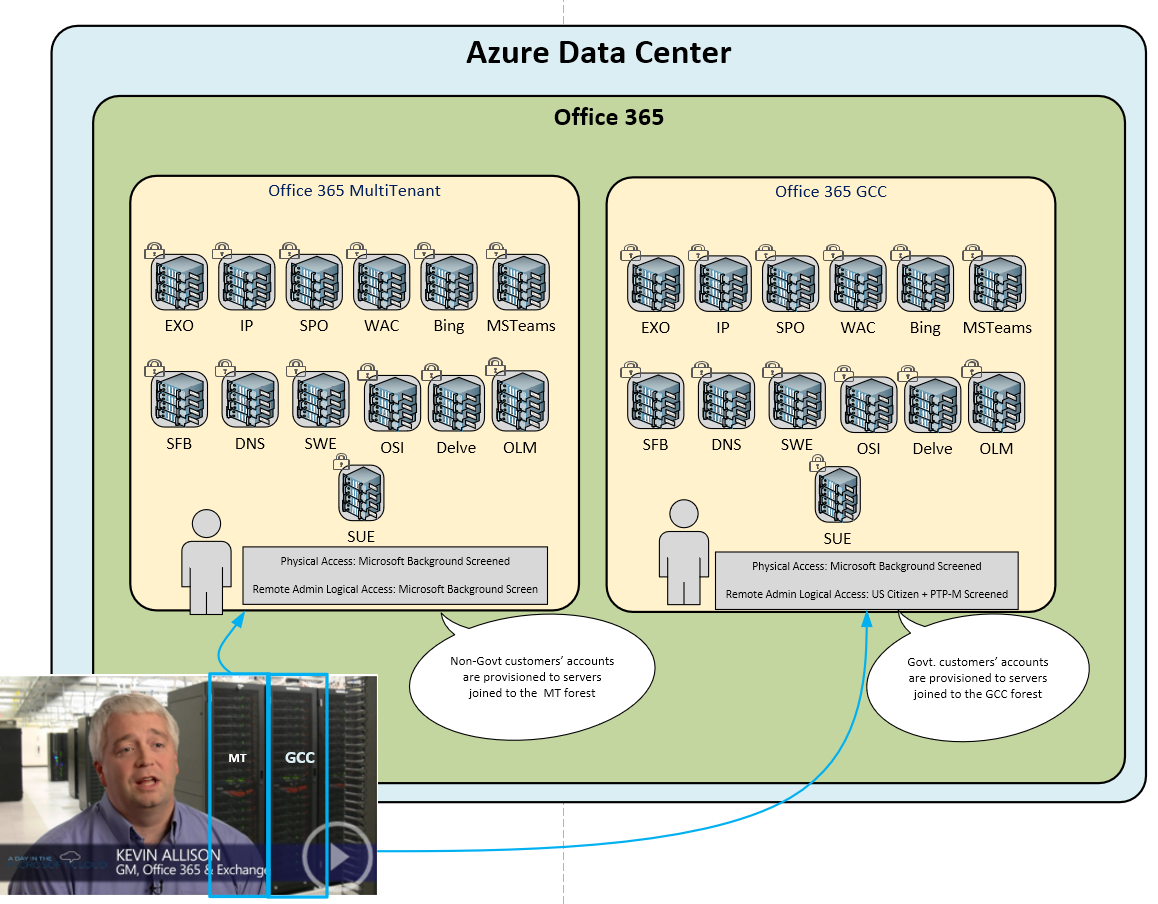


Figure 9‑ Office 365 MT and Office 365 GCC Separation Diagram

The above diagram shows separation of Office 365 MT and Office 365 GCC. The diagram shows that Office 365 GCC contains a separate version of the EXO, SPO, SFB, IP, WAC, SWE, SUE, OSI, Bing, DNS, Delve OLM, and MSTeams services with additional screening for Microsoft administrators with logical access. Restricted logical access is enforced by role-based access control (RBAC). Physical isolation is implemented via locked racks, as shown in the inset picture.

* 1. Information System Components and Boundaries

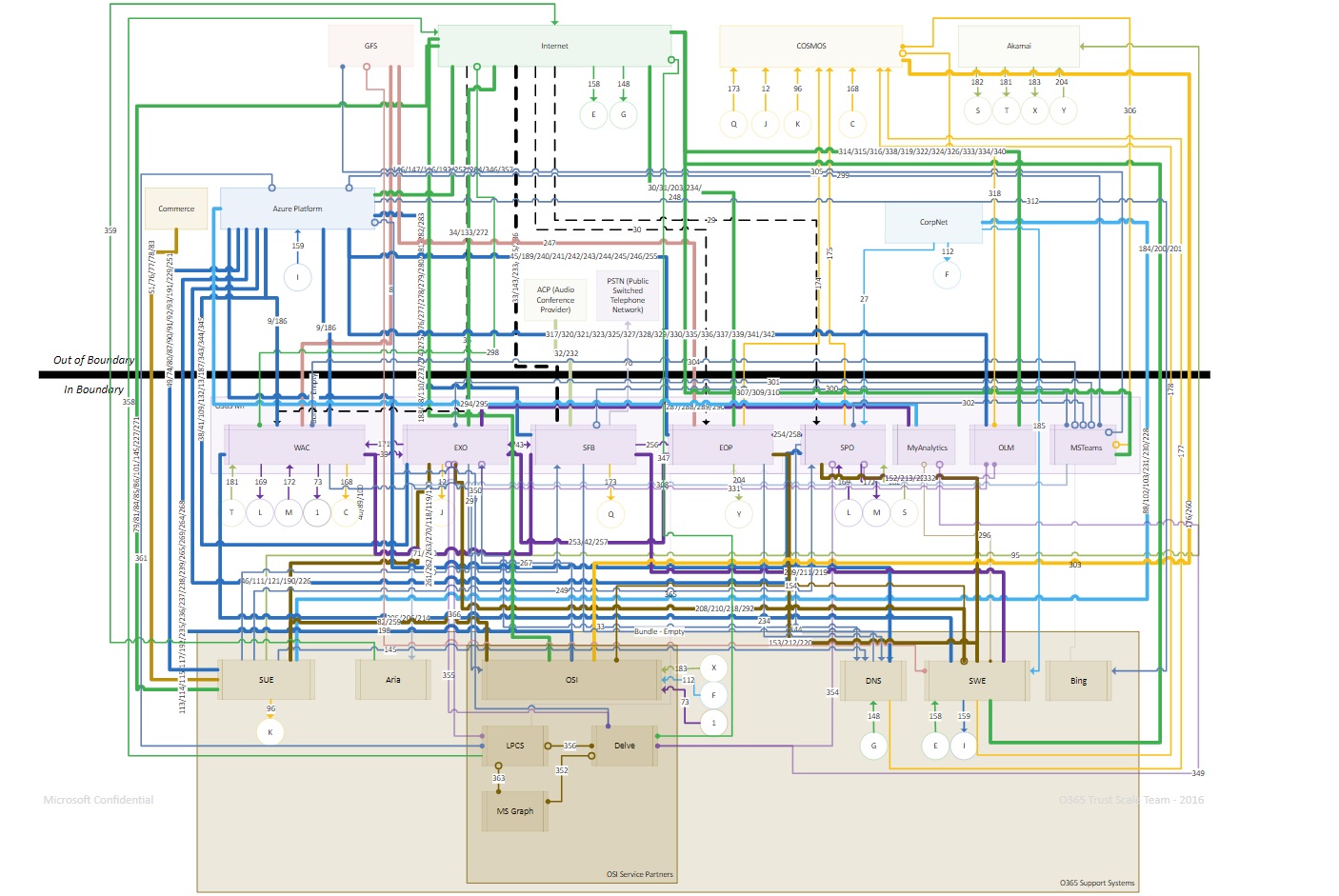
A detailed and explicit definition of the system authorization boundary diagram is represented in Figure 9‑2 Authorization Boundary Diagram below.

Figure ‑2 Authorization Boundary Diagram

As discussed in section 9.1, Office 365 MT is a major application that provides hosted Exchange Online, SharePoint Online, and Skype for Business services. The Office 365 MT FedRAMP boundary includes these services, as well as many other services that support these core, customer-facing services. A detailed description of each in-boundary service is included in section 9.5 of this SSP. Each service outside the boundary is described below. Interconnections with these services are protected via Interconnection Security Agreements (ISA); each agreement details the requirements necessary to protect the connection and the data shared via that connection equivalently to the protections within Office 365 MT; a brief summary of these protections is listed here.

**Azure** contains services used by Office 365 MT to host various aspects of the Office 365 MT service. The use of Azure is covered via an ISA. Connections to Azure services happen over FIPS 140-2 compatible TLS on specifically approved ports and protocols documented in ATTACHMENT 14 – Ports, Protocols and Services. These connections traverse the Azure network infrastructure where default-deny policies and other network protections are enforced. Specific controls inherited from Azure are listed in the Azure ISA. Azure has been granted a FedRAMP P-ATO.

**Akamai** represents the Global Traffic Manager (GTM) and Content Delivery Network (CDN) services run by Akamai Corporation on behalf of Office 365 MT. Akamai is used to distribute Office client software to end users. This use is protected via ISA with Akamai. No customer content is transmitted to Akamai or via Akamai. Interaction with this service is via API; the use of the API was developed in accordance with the Microsoft SDL process, which ensures that Office 365 MT does not rely on the external provider for security. Connections to Akamai happen over FIPS 140-2 compatible TLS on specifically approved ports and protocols documented in ATTACHMENT 14 – Ports, Protocols and Services. These connections traverse the Azure network infrastructure where default-deny policies and other network protections are enforced. No security controls are directly inherited from Akamai. Akamai has been granted a FedRAMP P-ATO.

**Geneva** is an extensible collection of libraries, tools and services that enable services to do Monitoring, Diagnostics and Analytics at scale. It is designed to support the requirements of all internal cloud services available on Azure and PilotFish environments. The Geneva System is part of the Cloud Engineering Services (CloudES) suite and active monitoring is offered to allow teams to build rich alerting. Geneva is a fully compliant offering (Azure and Office 365) and available in all national clouds.

**Cosmos** is a Microsoft service, not dedicated to Office 365 MT, that stores and reports on Office 365 MT log data. Office 365 MT scrubs logs of customer content before sending logs to Cosmos. Specifically, scrubbing takes fields containing customer content, encrypts or hashes that data, and replaces the field with the encrypted or hashed value. The rewritten log is sent to Cosmos, while each service team stores encryption keys as well as a mapping of hash keys to hashes within the Office 365 MT accreditation boundary. Cosmos can then correlate, alert, and report on these anonymized hashes. If an alert or report requires investigation, the logs are imported back inside the boundary. The service team can then repopulate the logs to their original state using the hash to key mapping. Because of the important nature of the Cosmos service, even though it does not store or process any customer content, it is expected that Cosmos security pertaining to protecting Office 365 MT will be assessed directly as part of FedRAMP accreditation auditing. Connections to Cosmos happen over FIPS 140-2 compatible TLS on specifically approved ports and protocols documented in ATTACHMENT 14 – Ports, Protocols and Services. These connections traverse the Azure network infrastructure where default-deny policies and other network protections are enforced. Specific controls inherited from Cosmos are listed in the Cosmos ISA.

**CorpNet** is a domain that contains services run on Microsoft’s corporate network, not dedicated to Office 365 MT, such as source code repositories, system documentation repositories, and change ticketing. These services are secured via ISA with CorpNet. No customer content is transmitted, processed or stored by CorpNet. Connections to these services happen via FIPS 140-2 compatible TLS on specifically approved ports and protocols documented in ATTACHMENT 14 – Ports, Protocols and Services. These connections traverse the Azure network infrastructure where default-deny policies and other network protections are enforced. No security controls are directly inherited from CorpNet.

TheSFB **PSTN** features require connectivity to the PSTN infrastructure to allow interaction between SFB and the PSTN. The Office 365 MT compliance boundary for PSTN features stops at the point where traffic is handed off to a PSTN carrier.

The Microsoft **Commerce** platform (Universal Store) manages direct customer communication and billing for Office 365. AAD pushes information to Commerce to facilitate billing and marketing for commercial clients. Only information necessary to facilitate billing and marketing is pushed to commerce; no other customer content is transmitted, processed, or stored by Commerce. Federal clients are billed through a separate solution and are not directly marketed to by the Microsoft Commerce division; federal customer information is deleted by the Commerce data collection process. These connections are shown for completeness. Connections to Commerce happen over FIPS 140-2 compatible TLS on specifically approved ports and protocols documented in ATTACHMENT 14 – Ports, Protocols and Services. Connections to these services happen via FIPS 140-2 compatible TLS on specifically approved ports and protocols documented in ATTACHMENT 14 – Ports, Protocols and Services. These connections traverse the Azure network infrastructure where default-deny policies and other network protections are enforced. No security controls are directly inherited from Commerce.

There is a connection between Office 365 Dedicated (a version of Office 365 not included in the accreditation boundary) and Office 365 MT. This connection exists so that Office 365 Dedicated can utilize certain Office 365 MT management servers. Information flow controls are in place to prevent the flow of any Office 365 MT data to Office 365 Dedicated and Office 365 MT does not depend on any controls implemented outside of Office 365 MT to maintain the confidentiality, integrity, and availability of Office 365 MT data with regard to this connection. This connection is documented here for completeness.

* 1. Types of Users

All personnel have their status categorized with a sensitivity level in accordance with PS-2. Personnel (employees or contractors) of service providers are considered Internal Users. All other users are considered External Users. User privileges (authorization permission after authentication takes place) are described in Table 9‑1 Personnel Roles and Privileges that follows.

Table ‑ Personnel Roles and Privileges

| Role | Internal or External | Privileged (P), Non-Privileged (NP), or No Logical Access (NLA) | Sensitivity Level | Authorized Privileges | Functions Performed |
| --- | --- | --- | --- | --- | --- |
| Customer User | External | N/A | N/A | N/A | Access Office 365 MT services |
| Customer Administrator | External | N/A | Limited | Customer portal administration | Administer customer user accounts, modify Office 365 MT service configurations |
| Service Engineer Operations | Internal | P | High-Risk | MT service production administrative access | Administer production Office 365 MT service |
| Service Engineer Operations (MT) | Internal | P | High-Risk | MT service production administrative access | Administer production Office 365 MT service |
| Program Manager | Internal | P | Moderate | Service team administrative access | Manages service team compliance |
| Developer | Internal | P | Moderate | Service team development environment access | Develops Office 365 MT |
| Tester | Internal | P | Moderate | Service team testing environment access | Tests Office 365 MT |
| Trust Program Manager | Internal | P | Limited | N/A | Responsible for compliance across all service teams, maintains compliance documentation |
| Office 365 Security Manager | Internal | P | Limited | N/A | Provides security governance and services, including vulnerability scanning, identity management, security incident response, audit collection and anti-virus and services, including vulnerability scanning, identity management, security incident response, audit collection and anti-virus |

The count of current users is proprietary information that is owned by Microsoft. The forecast of expected future customer users and internal administrators is proprietary information that is owned by Microsoft.

* 1. Network Architecture

The following Figure 9‑12 Network Diagram provides a visual depiction of how Office 365 MT integrates into the Azure network architecture.

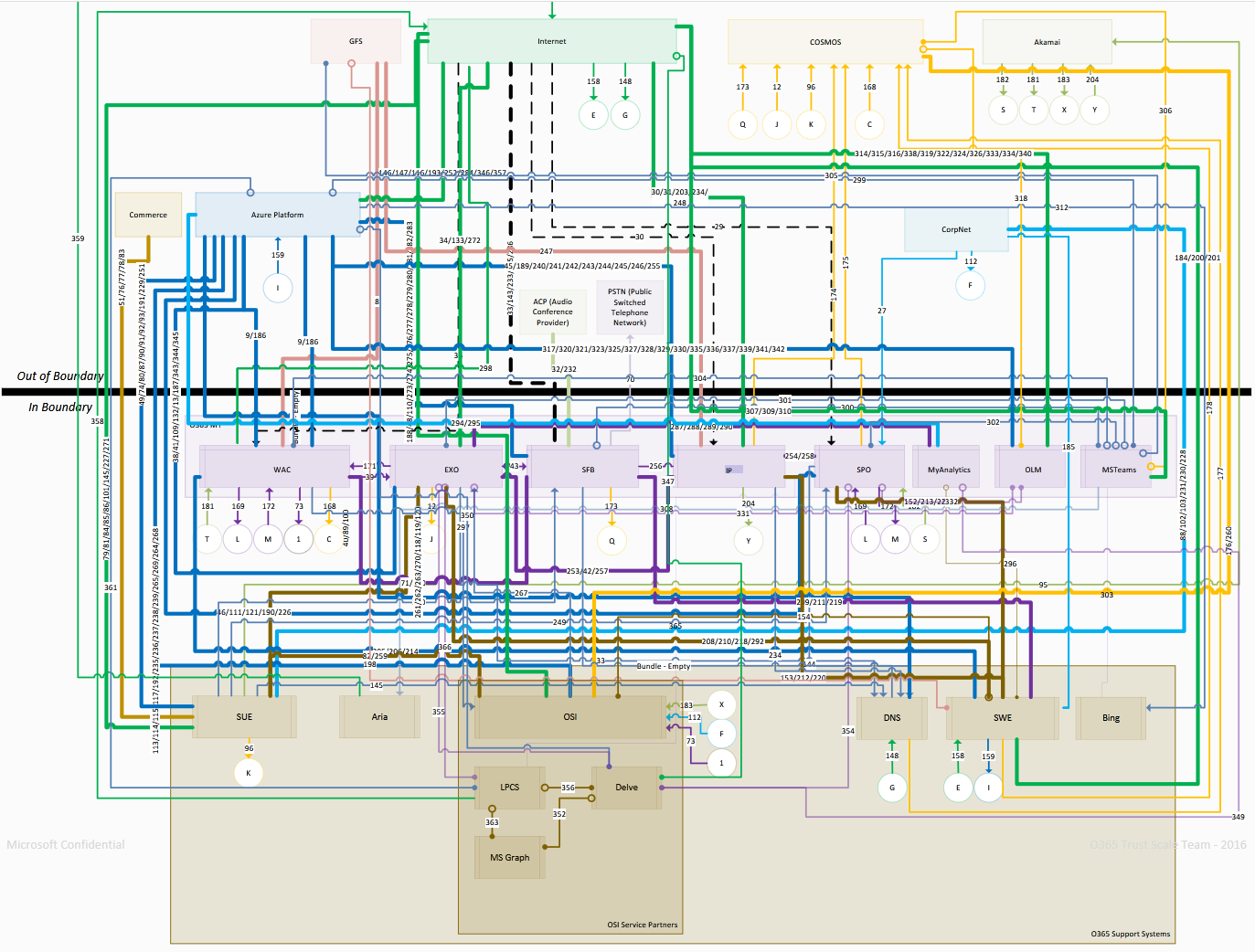


Figure ‑ Network Diagram

Office 365 MT leverages Azure for network infrastructure support, Data Center hosting, network operations, and physical/environmental controls. The Azure system accreditation boundary for FedRAMP consists of the Azure-managed domestic Data Centers (as outlined in the Azure SSP), the Azure core network infrastructure, the core servers providing critical shared services and management tools for the infrastructure, and the access network infrastructure that supports these critical core services. Office 365 MT servers are deployed into the area marked “Office 365 Authorization Boundary” on the bottom left of figure 9-2. These servers benefit from the same network protections and infrastructure as Azure’s core critical servers and Azure.

A complete listing of the Azure servers and network devices included in the Azure Accreditation Boundary can be found in the Azure Assessment & Authorization.

* 1. Service Description

A summary of the security environment for each service team is provided below, along with a service-team view of the data flows. An explanation of the full data flow can be found in section 9.2. Implementation details for all controls are found in section 13 of this SSP. The summaries in this section are intended to help the reader better understand the section 13 implementation details by providing background and context.

* + 1. Exchange Online (EXO)

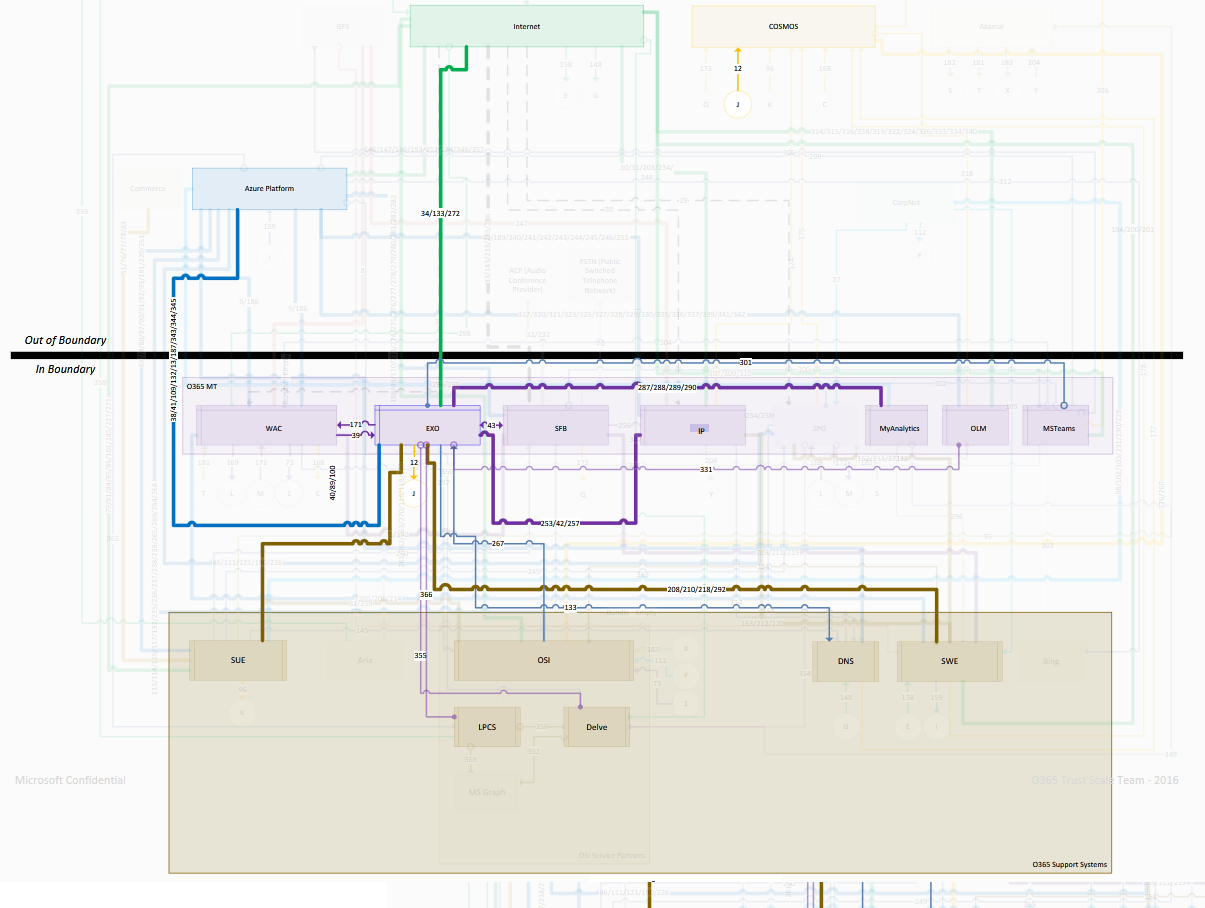


Figure 9‑3 Exchange Online Data Flows

Exchange Online (EXO) allows customers to access business email, calendar, and contacts on workstations, phones, and web browsers. The Exchange admin center provides an easy-to-use, web-based interface to manage their email services. Additionally, MyAnalytics on EXO helps customers build better work habits with personal productivity analytics.

EXO is hosted on physical servers within Azure data centers. These servers are joined to a security domain managed by EXO. Network access to these servers is controlled by Azure-owned and managed network devices using rules managed by EXO and approved by Office 365 MT. Azure also implements network intrusion detection and denial of service protection. There is an ACL-based default-deny policy in place between EXO servers and other service teams, Microsoft networks, and the internet. Only the flows, limited to specific ports and protocols and documented in the above data flow diagram and ATTACHMENT 14 – Ports, Protocols and Services of this SSP, are allowed.

Microsoft administrators access EXO through remote desktop gateways managed by SWE; this access requires smartcard based multifactor authentication.

Users interact with EXO via software email clients (e.g. Outlook) and webmail. Users’ access to customer content is based on claims information contained in tickets issued by AAD. The customer authenticates to their own ADFS infrastructure (as explained in section 9.1.3) which will issue a ticket that AAD will validate; AAD then issues an internal ticket. EXO reads this ticket and based on the username and groups within grants access to authorized mailboxes. No EXO customer content is sent outside of Office 365 MT other than to the customer and all customer interaction occurs over FIPS 140-2 compatible TLS (with the exception of customer-written emails sent to external email addresses). Customer content within EXO (i.e. email) is physically stored in Azure Continental United States (CONUS) data centers and in Office 365 MT-specific racks for Office 365 MT.

* + 1. SharePoint Online (SPO)

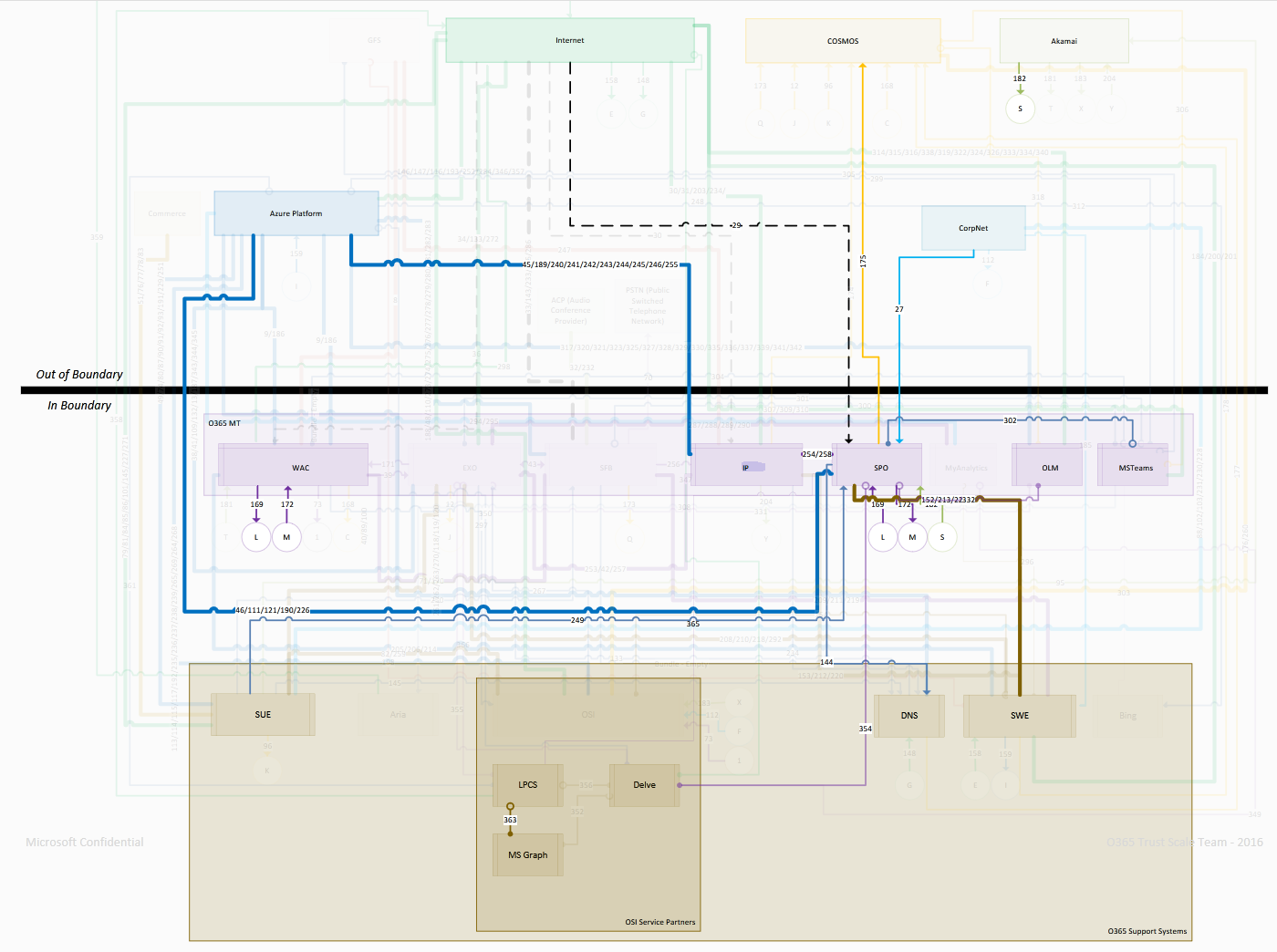


Figure ‑ SharePoint Online Data Flows

SharePoint Online (SPO) allows customers to share and manage content, knowledge, and applications to empower teamwork, quickly find information, and seamlessly collaborate across the organization.

SPO is hosted on physical servers within Azure data centers. These servers are joined to a security domain managed by SPO. Network access to these servers is controlled by Azure-owned and managed network devices using rules managed by SPO and approved by Office 365 MT. Azure also implements network intrusion detection and denial of service protection. There is an ACL-based default-deny policy in place between SPO servers and other service teams, Microsoft networks, and the internet. Only the flows, limited to specific ports and protocols and documented in the above data flow diagram and ATTACHMENT 14 – Ports, Protocols and Services of this SSP, are allowed.

Microsoft administrators access SPO through remote desktop gateways managed by SWE; this access requires smartcard based multifactor authentication.

Users interact with SPO through web browsers. The user authenticates to their own ADFS infrastructure which will issue a ticket that AAD will validate; AAD then issues an internal ticket. SPO reads the ticket and based on the username and groups within grants access to authorized SharePoint Online sites and files. No SPO customer content is sent outside of Office 365 MT other than to the customer and customer interaction occurs over FIPS 140-2 compatible TLS. Customer content within SPO (i.e. SharePoint Online pages) is physically stored in Azure Continental United States (CONUS) data centers and in Office 365 MT specific racks for Office 365 MT.

* + 1. Skype for Business (SFB)

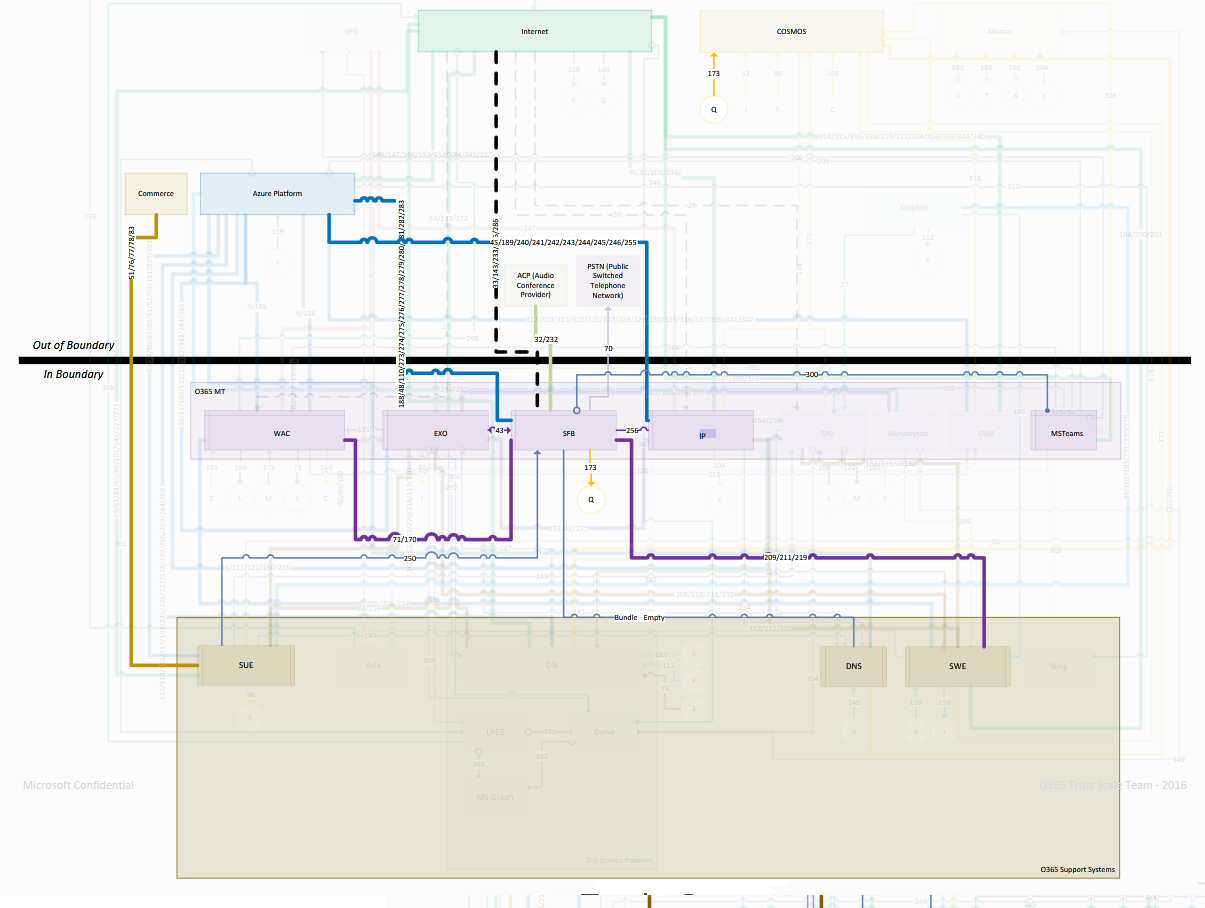


Figure ‑ Skype for Business Data Flows

Skype for Business (SFB) is a unified communications (UC) platform that integrates common channels of business communication and online meetings, including instant messaging (IM), presence, voice over IP (VoIP), voicemail, file transfers, video conferencing, web conferencing and email.

SFB is hosted on physical servers within Azure data centers, PaaS services on Azure, and uses Azure micro services such as Storage and Streaming Media.

The physical servers are joined to a security domain managed by SFB. Network access to these servers is controlled by Azure-managed network devices using rules managed by SFB and approved by Office 365 MT. Azure also implements network intrusion detection and denial of service protection. There is an ACL-based default-deny policy in place between SFB servers and other service teams, Microsoft networks, and the internet. Only the flows, limited to specific ports and protocols and documented in the above data flow diagram and ATTACHMENT 14 – Ports, Protocols and Services, are allowed.

The Azure PaaS services are hosted on VMs managed by Azure (as PaaS). There is an ACL-based default-deny policy in place for all virtual machines that only allows use of explicitly defined ports/protocols necessary for delivery of the service. Only the flows documented in the above data flow diagram and ATTACHMENT 14 – Ports, Protocols and Services, are allowed. Azure services accessed by API only are managed as part of the Azure compliance portfolio.

Microsoft administrators access SFB through remote desktop gateways managed by SWE; this access requires smartcard based multifactor authentication.

Users interact with SFB through the SFB client and web browsers. The user authenticates to their own ADFS infrastructure which will issue a ticket that AAD will validate; AAD then issues an internal ticket. SFB reads the ticket and based on the permissions grants access to authorized SFB sessions. Customer content is primarily handled internal to Office 365 services or on approved Azure services. All communications with the customer utilize FIPS 140-2 compatible TLS or SRTP protocols. When stored, customer calls, messages, voicemail and IM conversations are stored in EXO. Content uploaded to a meeting is stored (encrypted) on SFB servers only exists for the life of a meeting and will be deleted once the meeting ends. SFB physical servers resides in Azure CONUS data centers and in Office 365 MT-specific racks for Office 365 MT. The exception is Broadcast Meetings, which can store encrypted meetings on Azure CDN. For MT services, all Azure PAAS services consumed by SFB are hosted in the United States and are approved to handle data in accordance with the appropriate data handling standard.

SFB also offers public switched telephone network (PSTN) services like PSTN calling and PSTN conferencing. SFB PSTN services utilize existing SFB infrastructure and handle all data in accordance with Office 365 MT security controls. The Office 365 MT compliance boundary ends at the handoff of PSTN traffic to the PSTN provider. After the handoff PSTN traffic routes in accordance with telephony standards, and is outside the Office 365 MT compliance boundary.

* + 1. Office Online (WAC)

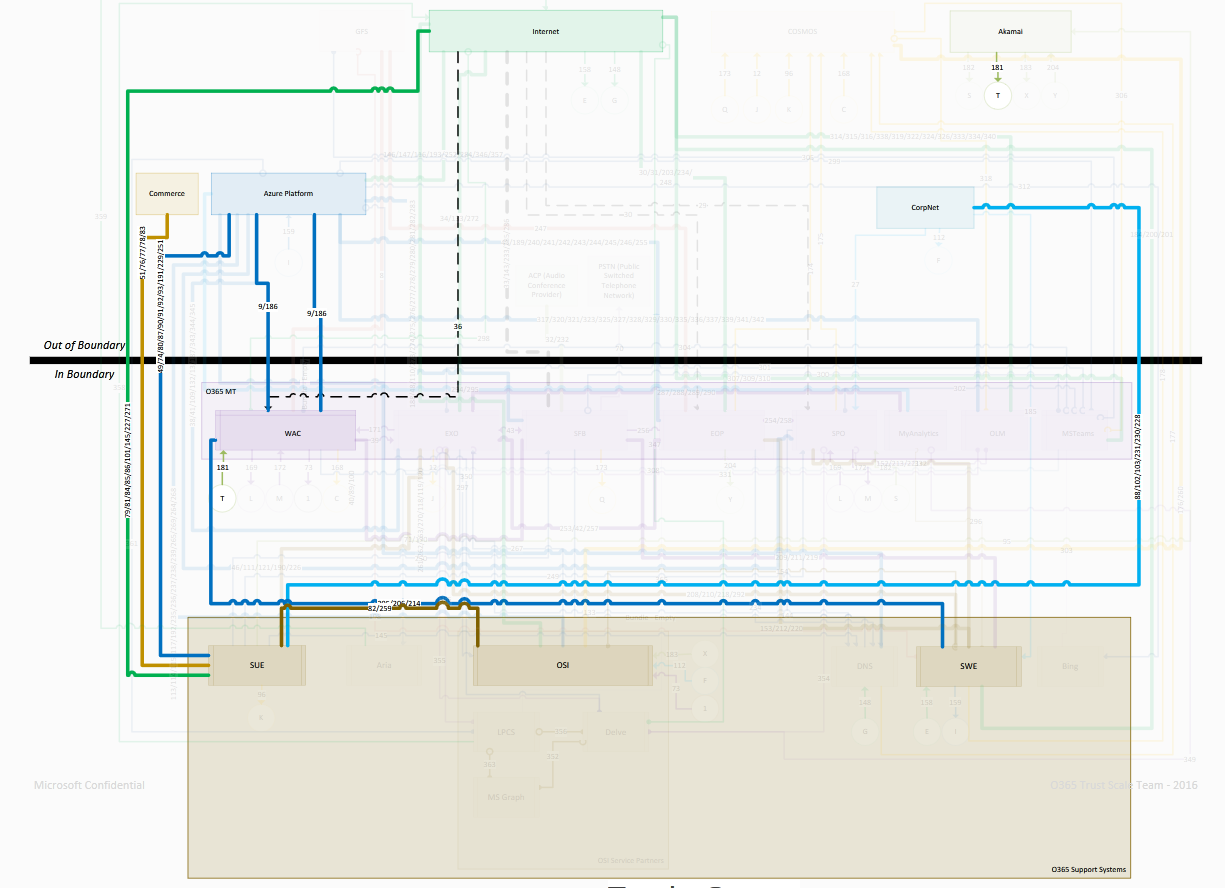


Figure 9‑7 Office Online Data Flows

Office Online (internally known as WAC) provides customers the ability to view and edit, via web browser, documents in Office 365. Examples include EXO attachments, SFB presentations, and SPO documents. Office Online also includes the Office Collaboration Service (OCS) that allows users to collaborate in real-time on SPO-hosted documents no matter which client the user is using (Desktop, Web, iPhone, Android).

Office Online is hosted on Azure IaaS VMs. These servers are joined to a security domain managed by Office Online. Network access to these servers is controlled using Azure Network Security Groups managed by Office Online and approved by Office 365 MT. Azure also implements network intrusion detection and denial of service protection. There is an ACL-based default-deny policy in place between Office Online servers and other service teams, Microsoft networks, and the internet. Only the flows, limited to specific ports and protocols and documented in the above data flow diagram and 10.2 of this SSP, are allowed.

Microsoft administrators access Office Online through remote desktop gateways managed by SWE; this access requires smartcard based multifactor authentication.

Users interact with Office Online; this interaction occurs via FIPS 140-2 compatible TLS. Documents viewed or edited in Office Online are subject to the same access restrictions that applied in EXO, SPO, or SFB. The user must first authenticate to EXO, SPO, or SFB which will then generate an access token which is sent to Office Online. Office Online passes that access token back to EXO, SPO, or SFB which validates it. Only valid tokens allow the user to view the requested content. No customer content is sent outside the system by Office Online other than to the customer, and although Office Online processes and temporarily caches customer content, Office Online is a stateless service and does not permanently store any customer content. Office Online physically resides in Azure CONUS regions.

* + 1. Security Workload Environment (SWE)

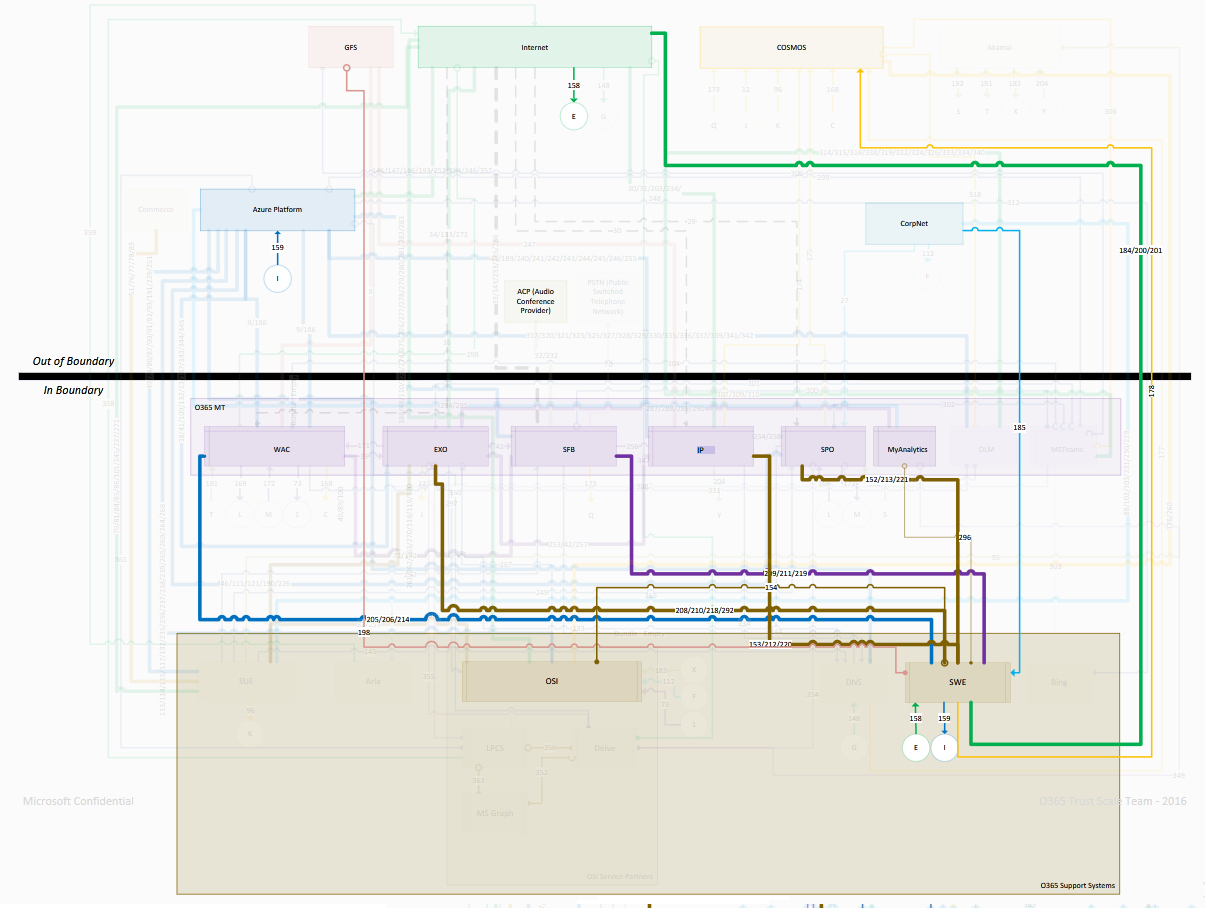


Figure 9‑8 Security Workload Environment Data Flows

Security Workload Environment (SWE) provides a security domain and a set of remote desktop gateways used by service teams.

SWE is hosted on physical servers within Azure data centers. These servers are joined to a security domain managed by SWE. Network access to these servers is controlled by Azure-managed network devices using rules managed by SWE and approved by Office 365 MT. Azure also implements network intrusion detection and denial of service protection. There is an ACL-based default-deny policy in place between SWE servers and other service teams, Microsoft networks, and the internet. Only the flows, limited to specific ports and protocols and documented in the above data flow diagram and ATTACHMENT 14 – Ports, Protocols and Services of this SSP, are allowed.

Microsoft administrators access SWE through remote desktop gateways managed by SWE; this access requires smartcard based multifactor authentication.

Customer users and customer administrators do not interact with SWE and SWE does not process or store any customer content. SWE physically resides in Azure CONUS data centers.

* + 1. Information Protection (IP)

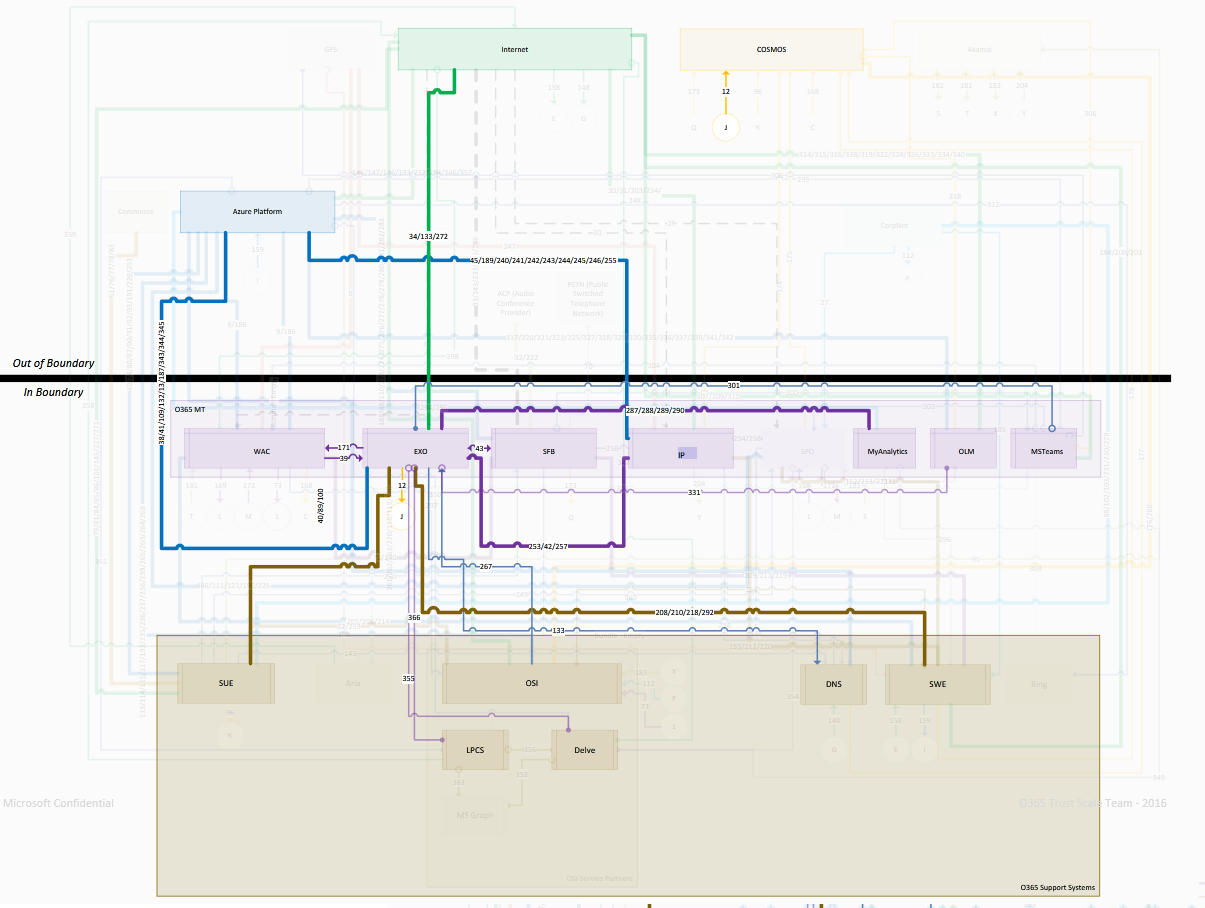


Figure ‑ Information Protection Data Flows

Information Protection (IP) provides anti-virus, anti-malware, and anti-spam filtering for email sent to Office 365 MT customers.

IP is hosted on physical servers within Azure data centers. These servers are joined to a security domain managed by EXO. Network access to these servers is controlled by Azure-managed network devices using rules managed by Azure and approved by Office 365 MT. Azure also implements network intrusion detection and denial of service protection. There is an ACL-based default-deny policy in place between IP servers and other service teams, Microsoft networks, and the internet. Only the flows, limited to specific ports and protocols and documented in the above data flow diagram and ATTACHMENT 14 – Ports, Protocols and Services of this SSP, are allowed.

Microsoft administrators access IP through remote desktop gateways managed by SWE; this access requires smartcard based multifactor authentication.

If enabled by customer administrators, users can interact with IP via web browser to configure spam filter sensitivity and mail routing rules. The user authenticates to their own ADFS infrastructure which will issue a ticket that AAD will validate; AAD then issues an internal ticket. IP reads the ticket and based on the username and groups grants access to view and modify the appropriate mail rules. Customer emails are processed but not stored by IP. No IP customer content is sent outside of Office 365 MT other than to the customer and customer interaction occurs over FIPS 140-2 compatible TLS. IP physically resides in Azure CONUS data centers and in Office 365 MT-specific racks for Office 365 MT.

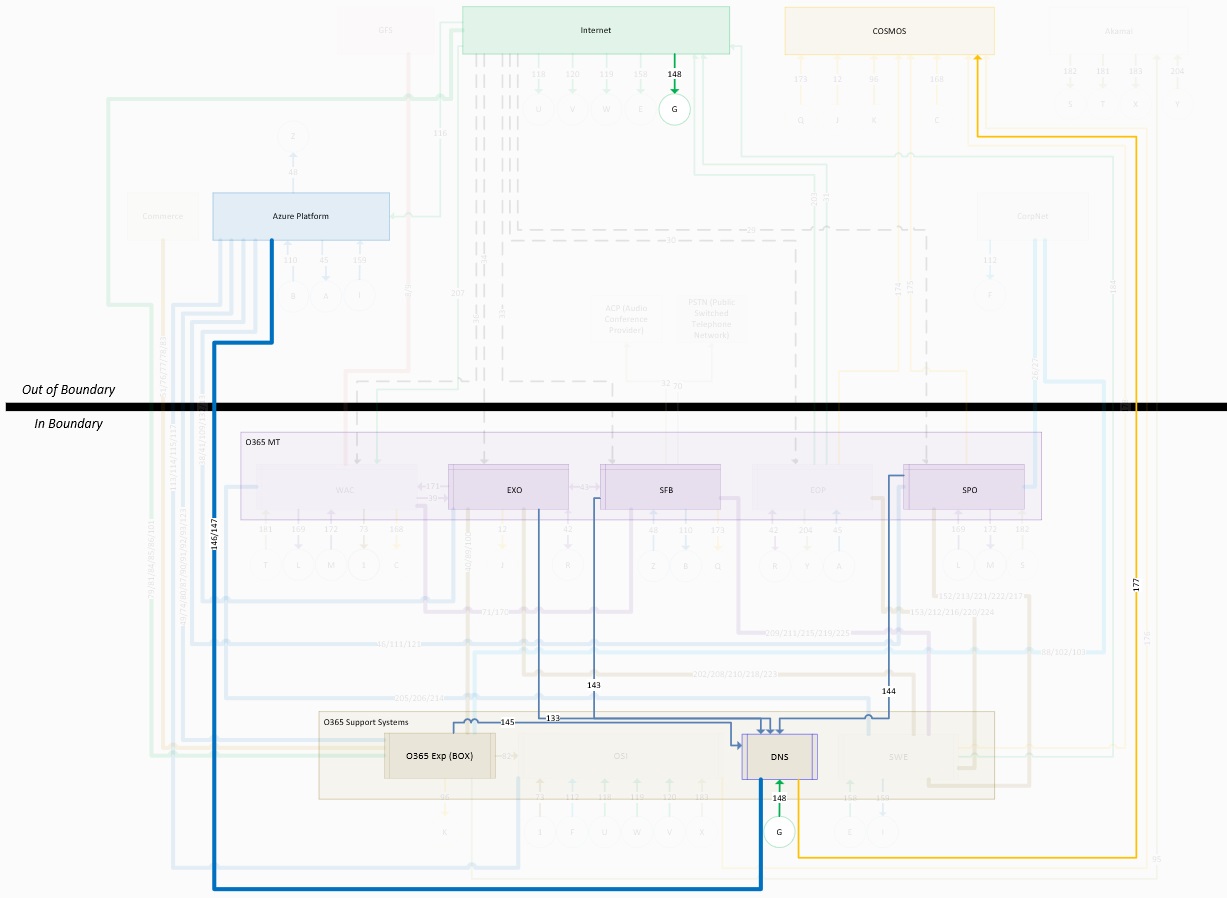
* + 1. Domain Name Service (DNS)

Figure ‑ DNS Data Flows

Domain Name Service (DNS) provides authoritative name resolution for some public facing domains associated with Office 365 MT. DNS also provides a suite of web services, available to customer administrators through a web interface, which allows modification of customer-specific subdomains.

DNS is hosted on physical servers within Azure data centers. These servers are joined to a security domain managed by Azure. Network access to these servers is controlled by Azure-managed network devices using rules managed by DNS and approved by Office 365 MT. Azure also implements network intrusion detection and denial of service protection. There is an ACL-based default-deny policy in place between DNS servers and other service teams, Microsoft networks, and the internet. Only the flows, limited to specific ports and protocols and documented in the above data flow diagram and ATTACHMENT 14 – Ports, Protocols and Services of this SSP, are allowed.

Microsoft administrators access DNS through PulseVPN managed by Azure; this access requires smartcard based multifactor authentication.

Customer administrator users interact with DNS via the portal, which is protected via FIPS 140-2 compatible TLS. The customer administrator authenticates to their own ADFS infrastructure which will issue a ticket that AAD will validate; AAD then issues an internal ticket. DNS reads the ticket and based on the username and groups grants access to modify customer-specific DNS records. These records are the only customer-specific data stored or processed within DNS. DNS physically resides in Azure CONUS data centers.

* + 1. Office 365 Suite User Experience (SUE)

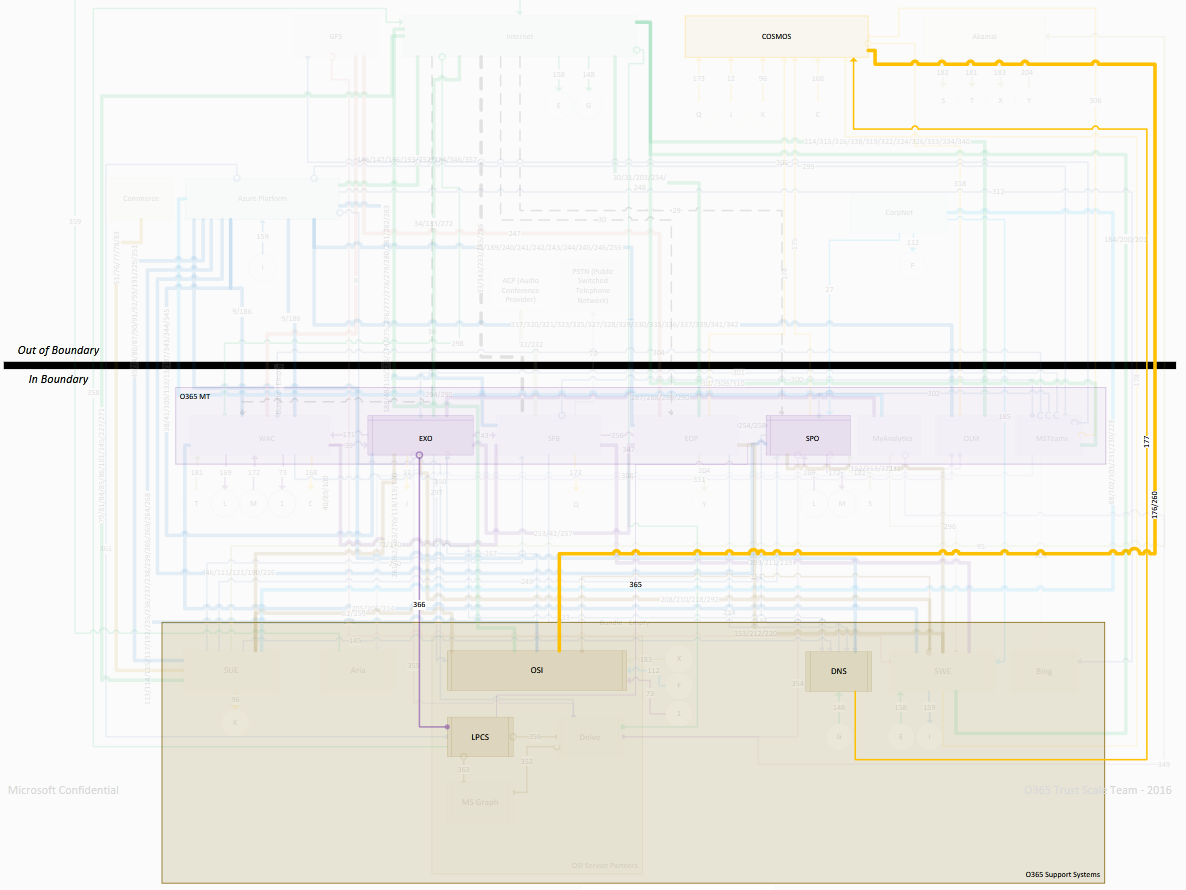


Figure ‑ Suite User Experience Data Flows

Suite User Experience (SUE) provides the web front end administrative interface for Office 365 MT, including SFB, EXO, and SPO. SUE also provides a web GUI for users to configure settings delegated to them by customer administrators. SUE also includes service health monitoring functionality used by service team administrators to monitor their services.

SUE is hosted on virtual servers managed by Azure. Network access to these servers is controlled by Azure devices using rules managed by SUE and approved by Office 365 MT. Azure is responsible for implementation of network intrusion detection and denial of service protection. There is an ACL-based default-deny policy in place between SUE virtual machines and other service teams, Microsoft networks, and the internet. Only the flows, limited to specific ports and protocols and documented in the above data flow diagram and ATTACHMENT 14 – Ports, Protocols and Services of this SSP, are allowed.

Microsoft administrators do not access SUE virtual machines directly. They manage the service via the Azure Administrative Portal run by Azure. This access requires smartcard based multifactor authentication.

Users interact with SUE when accessing SFB, EXO, and SPO administration portals via web browser; these interactions are protected by FIPS 140-2 compatible TLS. SUE is a stateless service and does not store any customer content. SUE is deployed on Azure instances located in Azure CONUS data centers.

* + 1. Office Service Infrastructure (OSI)

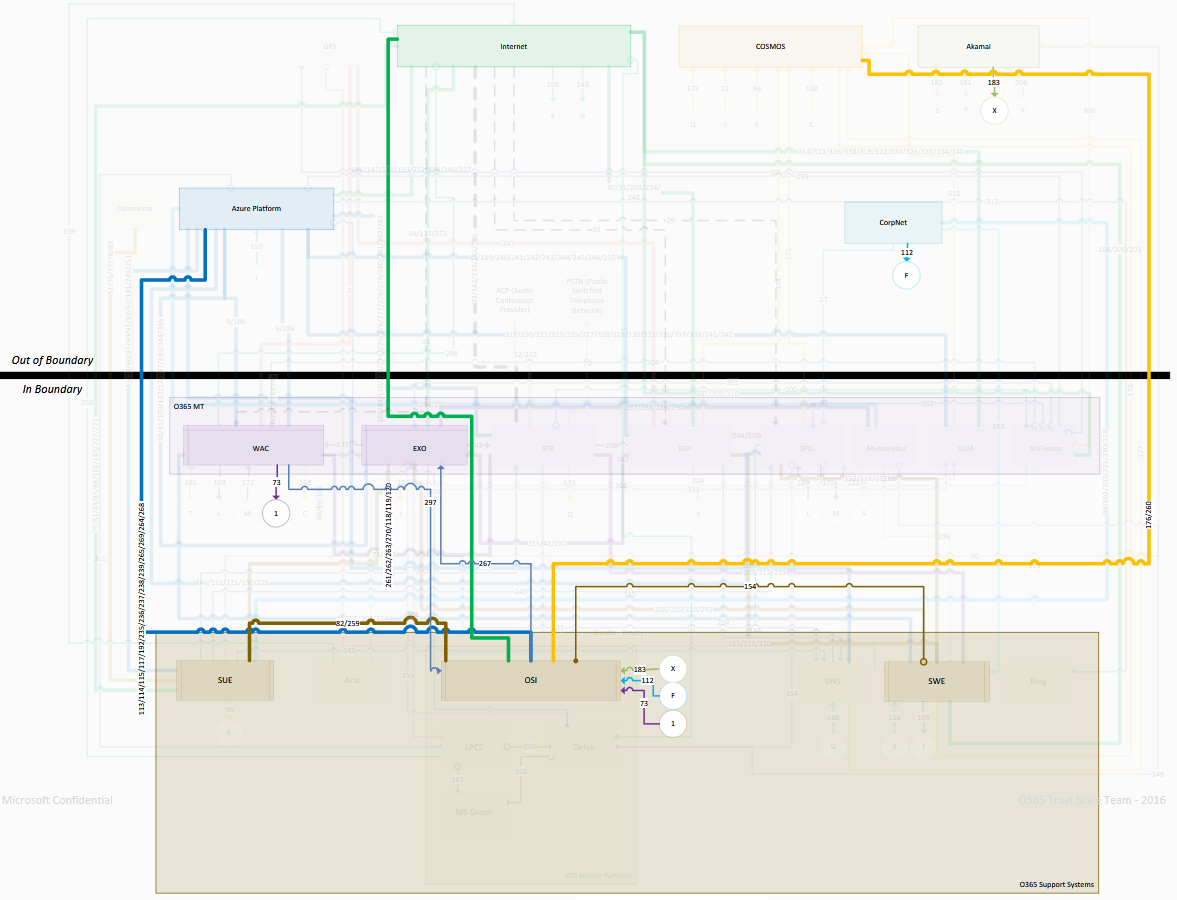


Figure ‑ Office Service Data Flows

Office Service Infrastructure (OSI) provides a platform for backend applications that enhance the overall Office 365 MT service offering. OSI and its application partners are hosted on Azure and contain deployment, hosting and monitoring infrastructure applications which include services as Forms, Planner, Click2Run, Office Licensing Service, and Roaming, etc.

OSI and the partners hosted on OSI use virtual servers managed by Azure. Network access to these servers is controlled by Azure devices using rules managed by OSI and approved by Office 365 MT. Azure provides the implementation of network intrusion detection and denial of service protection. There is an ACL-based default-deny policy in place between SUE virtual machines and other service teams, Microsoft networks, and the internet. Only the flows, limited to specific ports and protocols and documented in the above data flow diagram and ATTACHMENT 14 – Ports, Protocols and Services of this SSP, are allowed.

Microsoft administrators access OSI provisioned virtual machines via Remote Desktop. This process requires enabling an account with a random password and then connecting using that account. This process is gated by two-factor authentication. Users do not interact with OSI and OSI does not store customer content. Connections between Office applications or SUE and OSI occur over FIPS 140-2 compatible TLS. Azure is responsible for ensuring that OSI virtual machines are provisioned in Azure CONUS data centers.

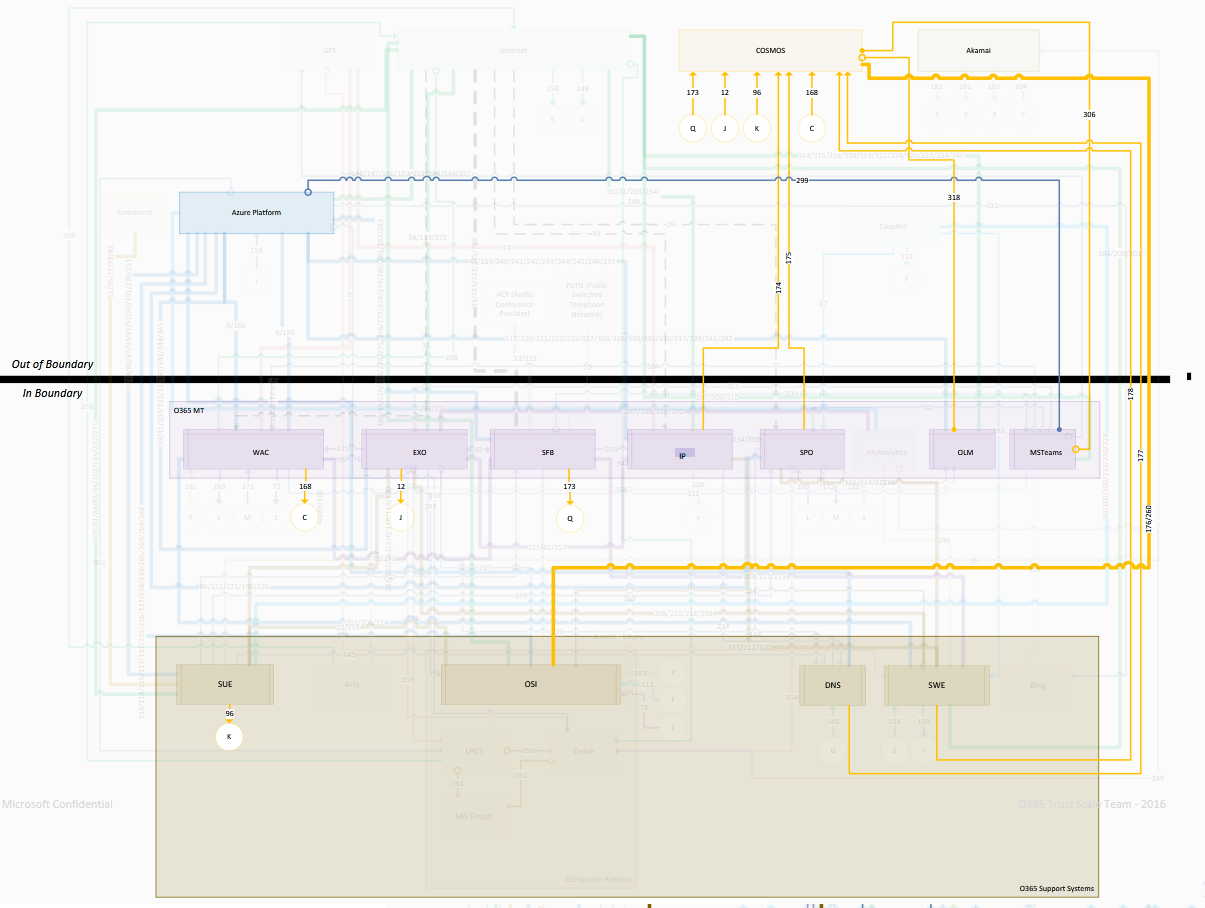
* + 1. Azure Active Directory (AAD)

Figure 9‑12 Azure Active Directory Data Flows

Azure Active Directory (AAD) supports customer authentication, but is not part of the Office 365 MT Support accreditation boundary. Azure Active Directory provides a single-sign-on identity and access management solution along with a robust set of tools to manage users and groups. This solution provides secure access to the Office 365 online services. Full details of AAD’s security architecture and control implementations can be found in the Microsoft Azure SSP. AAD contains backend services which provide user account management, including the services that support ADFS as described in section 9.1.3.

Customers are required to enable Active Directory Federation Services (ADFS) to manage their users’ identities and authorizations. Users do not interact with AAD directly. Connections between AAD and the customer’s Active Directory infrastructure are protected via FIPS-compliant TLS.

* + 1. Microsoft Teams (MSTeams)

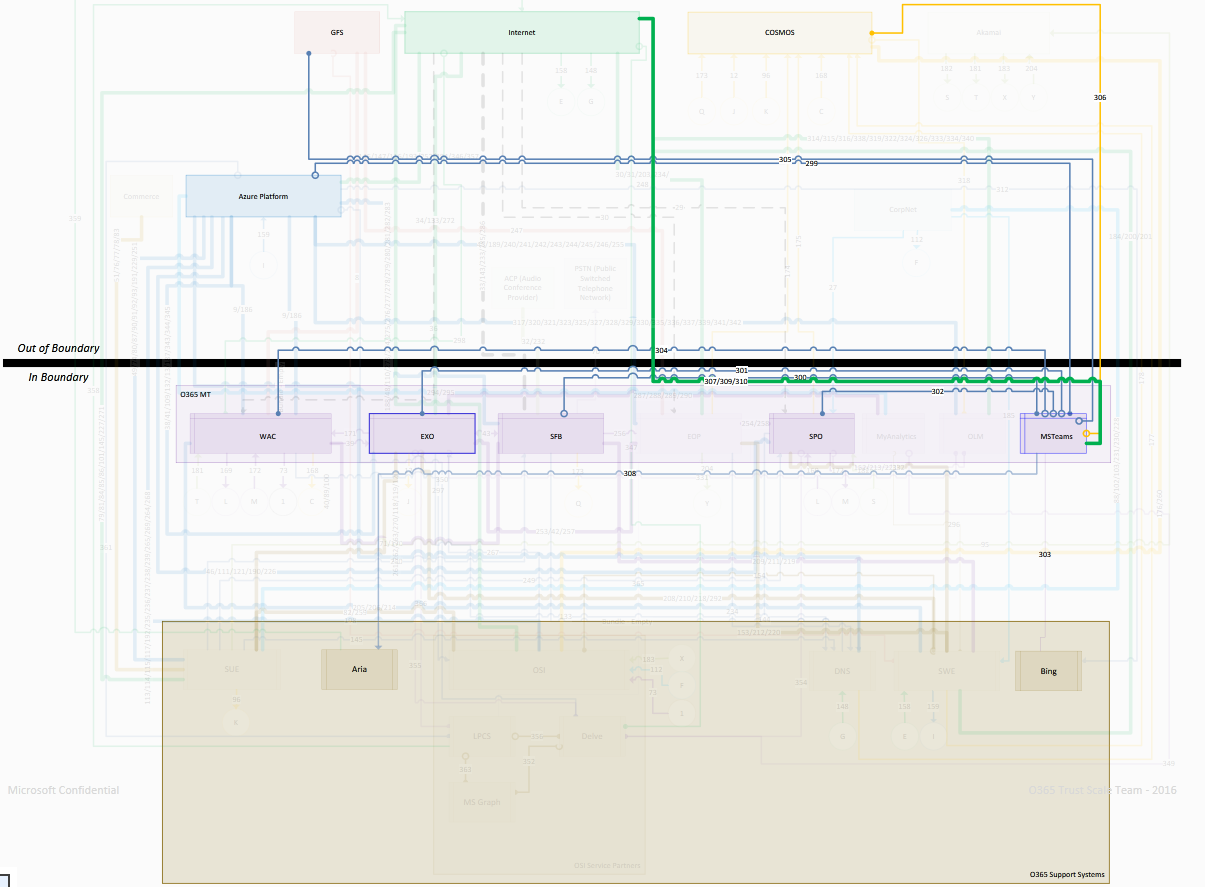


Figure 9‑13 Microsoft Teams Data Flows

Microsoft Teams (MSTeams) is an immersive workspace solution that provides instant messaging and group chat, voice/video calling and conferencing, file sharing, and shared workspace. Microsoft administrators access MSTeams through remote desktop gateways managed by SWE; this access requires smartcard based multifactor authentication.

MSTeams is hosted on physical servers within Azure data centers managed by Azure and use the Azure PilotFish service, as well as Azure micro services such as Storage and Streaming Media. The physical servers may be joined to a security domain managed by Azure. Network access to these servers is controlled by Azure-managed network devices using rules managed by Skype organization and approved by Office 365 MT. Azure also implements network intrusion detection and denial of service protection. All Azure based services are hosted on VMs, or hardware managed by Azure. There is an ACL-based default-deny policy in place for all virtual machines that only allows use of explicitly defined ports/protocols necessary for delivery of the service. Only the flows documented in the above data flow diagram and section 9.5 of this SSP, are allowed. Azure services accessed by API only are managed as part of the Azure compliance portfolio.

Users interact with MSTeams through the MSTeams client and web browsers. The user authenticates to their own ADFS infrastructure which will issue a ticket that AAD will validate; AAD and MSTeams then issue internals tickets to be used to access various components. MSTeams reads the ticket and based on the permissions grants access to authorized MSTeams resources. Customer content is primarily handled internal to Office 365 services or on approved Azure services. All communications with the customer utilize FIPS 140-2 compatible protocols. When stored, customer calls, messages, voicemail and IM conversations are stored in EXO, Azure storage, or Object Store. Content uploaded to MSTeams is stored in SharePoint Online. For MT services, all Azure PaaS services consumed by MSTeams that handle content or EUII are hosted in the United States and are approved to handle data in accordance with the appropriate data handling standard.

* + 1. Bing

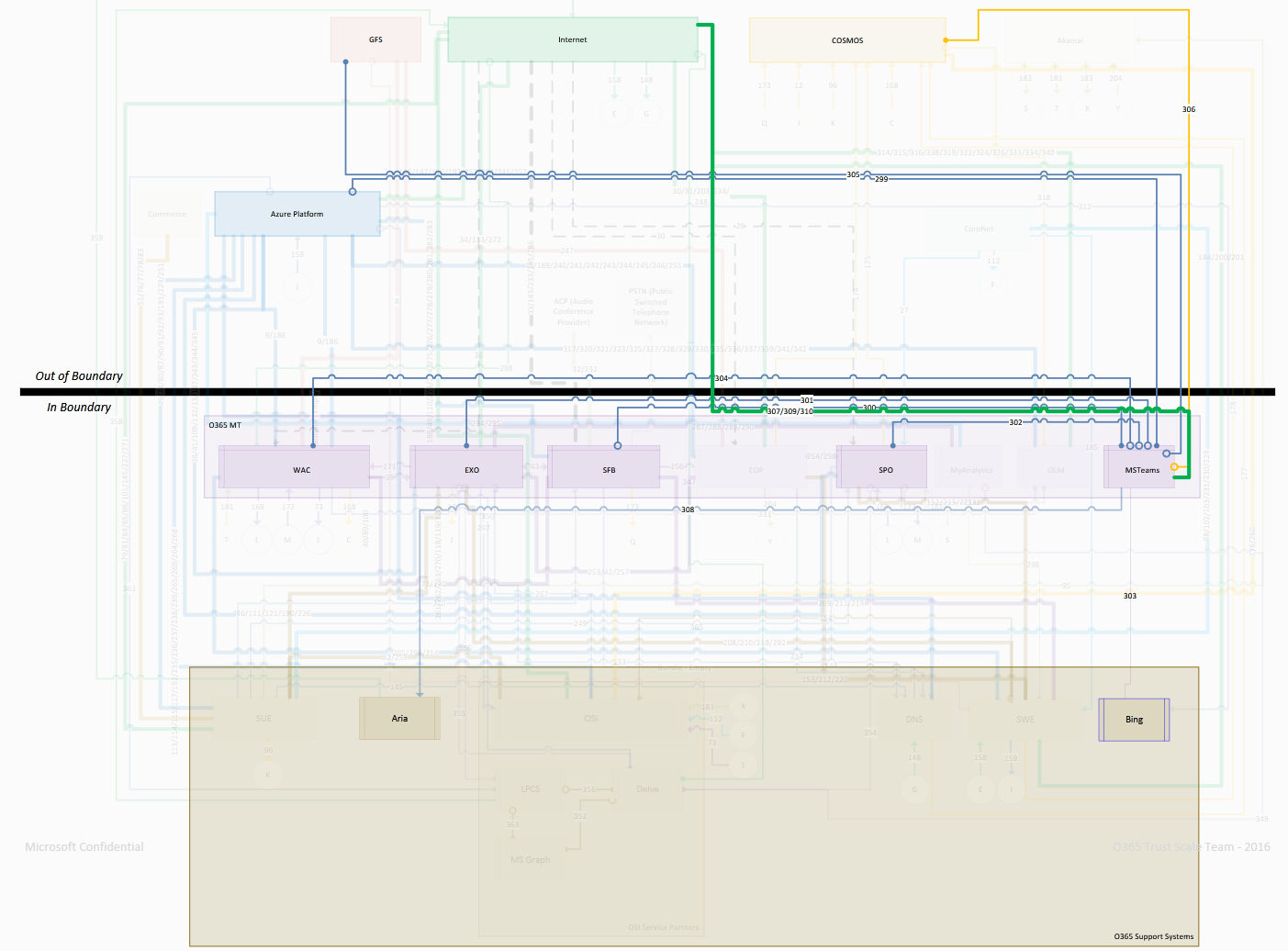


Figure 9‑14 Bing Data Flows

The Bing service consists of several first party, backend services (Object Store, Siphon, QAS, Aria, and Speller) designed to support customer facing Office 365 services.

Connections with Bing teams occur over FIPS 140-2 compliant TLS. Additionally, customer content stored by Bing teams are encrypted with a FIPS 140-2 compliant algorithm. Users do not directly interact with customer content stored by Bing.

Some Bing teams are hosted on servers managed by PilotFish. This includes the management of baseline configurations and hardware components. Additionally, PilotFish provides antivirus scanning as well as BeyondTrust vulnerability scanning. There is an ACL-based default-deny policy in place between Bing servers and other service teams, Microsoft networks, and the internet.

K9 is the security monitoring capability is provided through PilotFish. K9 is used by some teams to collect, store and perform real-time analysis on security logs to flag suspected intrusions or unusual activity. Bing teams coordinate with both PilotFish and the Office 365 Security and Incident Response teams on events requiring further investigation.

Microsoft administrators access Bing teams through remote desktop gateways managed by SWE; this access requires smartcard based multifactor authentication.

* + 1. Outlook Mobile (OLM)



Figure 9‑15 Outlook Mobile Data Flows

Outlook Mobile is a client that is built to function on iOS and Android platforms (as well as interfacing with Exchange Online) using the Outlook Mobile Service (OMS). Outlook Mobile accomplishes several roles including API translation, Notifications, Device Management, and Value add services. Outlook Mobile also serves as a middle tier for other email providers for which it performs some mailbox caching.

Outlook Mobile is hosted on Microsoft Azure; Microsoft administrators do not access Azure virtual machines directly. Administrators access the service through gateways; this access requires multifactor authentication. Network access to these servers is controlled by Azure-managed network devices and approved by Office 365 MT. Azure also implements network intrusion detection and denial of service protection. There is an ACL-based default-deny policy in place with service teams, Microsoft networks, and the internet.

* + 1. Delve

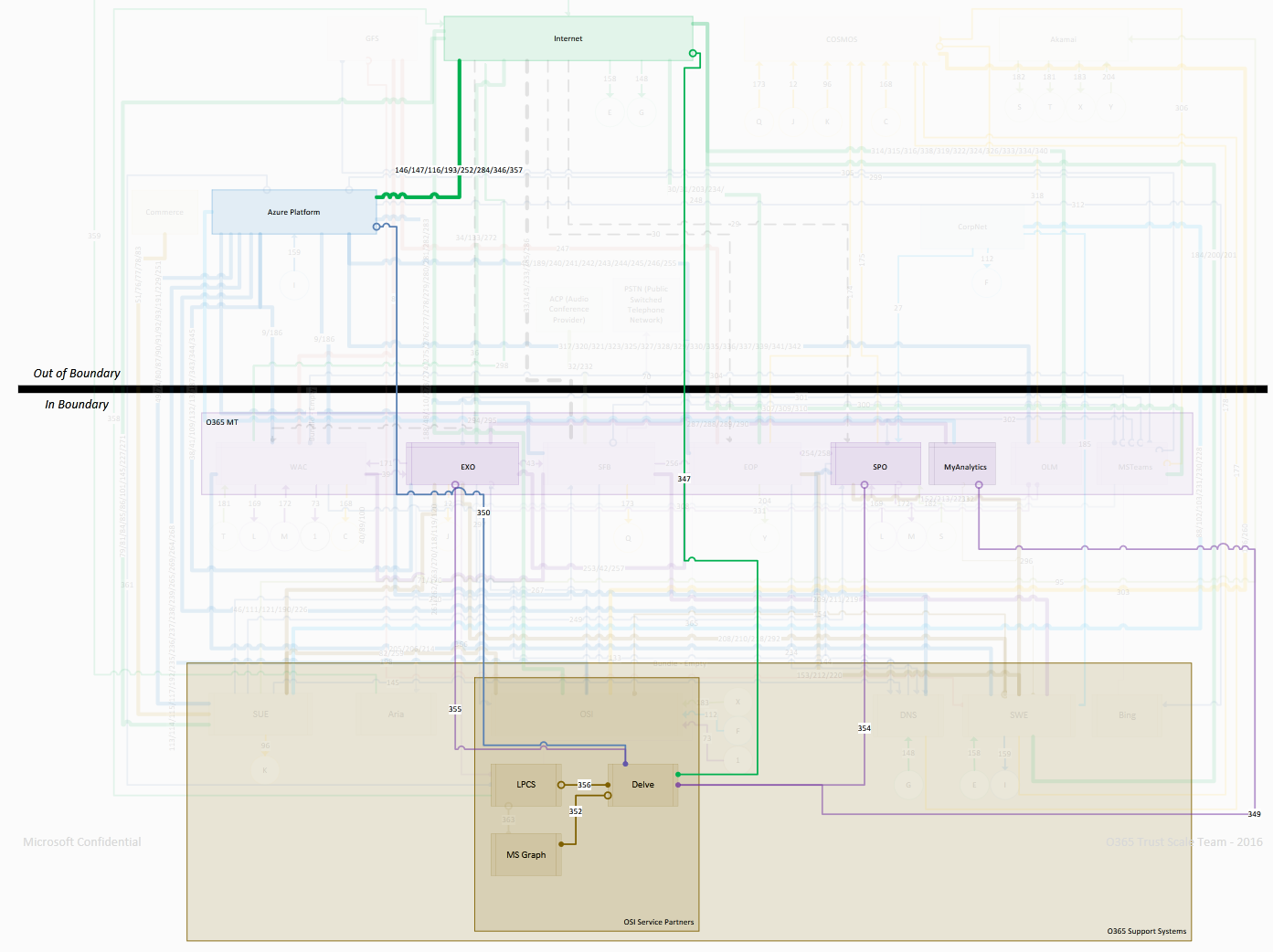


Figure 9‑16 Delve Data Flows

Delve allows customers to manage their Office 365 profile, and to discover and organize the information that's likely to be most interesting across Office 365. Delve determines the relevancy of information based on the user's relationships as well as activity within the user’s organization.

Delve encompasses Loki (Live Persona Card Service), a backend service used to power Live Persona Cards. The Live Persona Cards are displayed to customers on mouse over and deliver personalized and contextual information based on the workload.

Delve is hosted on Azure virtual servers. Network access to these servers is controlled by Azure devices using rules managed by Delve and approved by Office 365 MT. Azure is responsible for implementation of network intrusion detection and denial of service protection. There is a default-deny network access policy in place between Delve virtual machines and other service teams, Microsoft networks, and the internet. Only the flows, limited to specific ports and protocols and documented in the above data flow diagram and ATTACHMENT 14 – Ports, Protocols and Services of this SSP, are allowed.

Microsoft administrators do not access Delve virtual machines directly. Administrators access the service through a “jump box” VM in the Delve environment and remote desktop gateways managed by SWE; this access requires smartcard based multifactor authentication.

Customers interact with Delve via web browser protected by FIPS 140-2 compatible TLS. Delve is deployed on Azure instances located in Azure CONUS data centers.

1. System Environment And Inventory

Directions for attaching the FedRAMP Inventory Workbook may be found in the following section: ATTACHMENT 13 – FedRAMP Inventory Workbook.

* 1. Data Flow

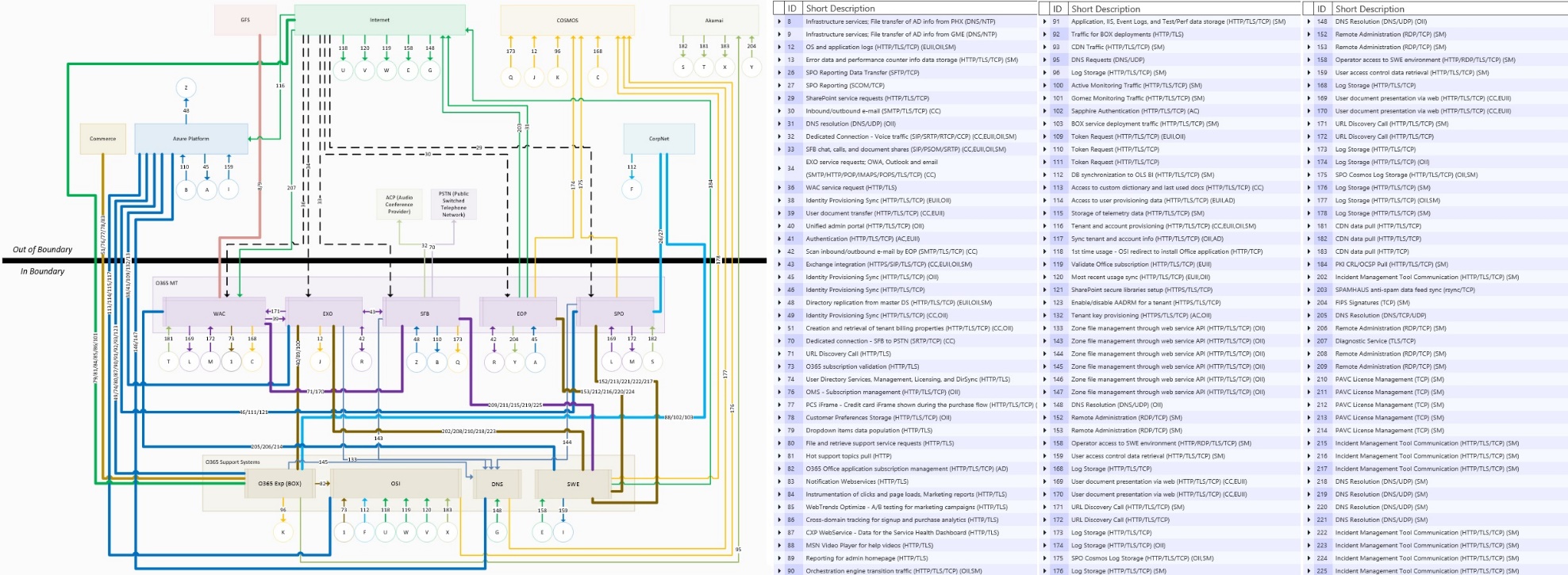
The data flow in and out of the system boundaries is represented in diagrams below.

Figure 10‑1 Data Flow Diagram

The above diagram and accompanying legend documents all data flows between Office 365 MT service teams, between Office 365 MT and interconnected systems, and between Office 365 MT and customers. The data flows involving customer content are discussed here in narrative format, but detailed information about each flow, including source and destination, is available from Microsoft provided appropriate confidentiality agreements are in place.

* 1. Ports, Protocols, and Services

Due to the scale of the Microsoft Office 365 MultiTenant environment, the Ports, Protocols, and Services table is provided in Attachment 14 – Ports & Protocols.

1. System Interconnections

The Table 11‑1 System Interconnections below is consistent with Table 13‑3 CA-3 Authorized Connections.

Table 11‑1 System Interconnections

| Service Processor IP Address and Interface | External Organization Name and IP Address of System | External Point of Contact and Phone Number | Connection Security (IPSec VPN, TLS, Certificates, Secure File Transfer, etc.)\* | Data Direction  (incoming, outgoing, or both) | Information Being Transmitted | Port or Circuit Numbers |
| --- | --- | --- | --- | --- | --- | --- |
| N/A | Core Services Engineering (CSE, formerly MSIT) CorpNet | Lisa Reshaur  (425) 703-1935 | TLS | Both | System Documentation, build information, change ticketing | N/A |
| N/A | Azure | Tom Keane  425-241-1298 | TLS | Both | System data | N/A |
| N/A | Cosmos | Ryan Waite  (425) 706-1894 | TLS | Both | Scrubbed log data | N/A |
| N/A | Office 365 Support | Elisabeth Zornes  (415) 229-0349 | TLS | Both | Basic account information | N/A |
| N/A | Universal Store | Doug Taylor  (425) 707-4908 | TLS | Both | Commercial Customer Billing Information | N/A |
| N/A | Akamai | Tom Ruff  (703) 621-4027 | TLS | Both | DNS info, static website content | N/A |

\*Internet Protocol Security (IPSec), Virtual Private Network (VPN), Transport Layer Security (TLS)

1. Laws, Regulations, Standards and Guidance

A summary of FedRAMP Laws and Regulations is included in ATTACHMENT 12 – FedRAMP Laws and Regulations.

* 1. Applicable Laws and Regulations

The FedRAMP Laws and Regulations can be found on this web page: [Templates](https://www.fedramp.gov/resources/templates-2016/).

Table 12‑1 Office 365 MultiTenant Cloud Laws and Regulations includes additional laws and regulations specific to Office 365 MultiTenant.

Table 12‑1 Office 365 MultiTenant Cloud Laws and Regulations

|  |  |  |  |
| --- | --- | --- | --- |
| Identification Number | Title | Date | Link |
|  | N/A |  |  |
|  |  |  |  |
|  |  |  |  |

* 1. Applicable Standards and Guidance

The FedRAMP Standards and Guidance be found on this web page: [Templates](https://www.fedramp.gov/resources/templates-2016/)

Table 12‑2 Office 365 MultiTenant Cloud Standards and Guidance includes in this section any additional standards and guidance specific to Office 365 MultiTenant Cloud.

Table 12‑2 Office 365 MultiTenant Cloud Standards and Guidance

|  |  |  |  |
| --- | --- | --- | --- |
| Identification Number | Title | Date | Link |
|  | N/A |  |  |
|  |  |  |  |
|  |  |  |  |

1. Minimum Security Controls

Security controls must meet minimum security control baseline requirements. Upon categorizing a system as Low, Moderate, or High sensitivity in accordance with FIPS 199, the corresponding security control baseline standards apply. Some of the control baselines have enhanced controls which are indicated in parentheses.

Security controls that are representative of the sensitivity of Office 365 MT are described in the sections that follow. Security controls that are designated as “Not Selected” or “Withdrawn by NIST” are not described unless they have additional FedRAMP controls. Guidance on how to describe the implemented standard can be found in NIST 800-53, Rev 4. Control enhancements are marked in parentheses in the sensitivity columns.

Systems that are categorized as FIPS 199 Low use the controls designated as Low, systems categorized as FIPS 199 Moderate use the controls designated as Moderate and systems categorized as FIPS 199 High use the controls designated as High. A summary of which security standards pertain to which sensitivity level is found in Table 13‑1 Summary of Required Security Controls that follows.

Table 13‑1 Summary of Required Security Controls

| ID | Control Description | Sensitivity Level | | | |
| --- | --- | --- | --- | --- | --- |
| Low | | Moderate | High |
| AC | Access Control |  | |  |  |
| AC-1 | Access Control Policy and Procedures | AC-1 | | AC-1 | AC-1 |
| AC-2 | Account Management | AC-2 | | AC-2 (1) (2) (3) (4) (5) (7) (9) (10) (12) | AC-2 (1) (2) (3) (4) (5) (7) (9) (10) (11) (12) (13) |
| AC-3 | Access Enforcement | AC-3 | | AC-3 | AC-3 |
| AC-4 | Information Flow Enforcement | Not Selected | | AC-4 (21) | AC-4 (8) (21) |
| AC-5 | Separation of Duties | Not Selected | | AC-5 | AC-5 |
| AC-6 | Least Privilege | Not Selected | | AC-6 (1) (2) (5) (9) (10) | AC-6 (1) (2) (3) (5) (7) (8) (9) (10) |
| AC-7 | Unsuccessful Logon Attempts | AC-7 | | AC-7 | AC-7 (2) |
| AC-8 | System Use Notification | AC-8 | | AC-8 | AC-8 |
| AC-10 | Concurrent Session Control | Not Selected | | AC-10 | AC-10 |
| AC-11 | Session Lock | Not Selected | | AC-11 (1) | AC-11 (1) |
| AC-12 | Session Termination | Not Selected | | AC-12 | AC-12 (1) |
| AC-14 | Permitted Actions Without Identification or Authentication | AC-14 | | AC-14 | AC-14 |
| AC-17 | Remote Access | AC-17 | | AC-17 (1) (2) (3) (4) (9) | AC-17 (1) (2) (3) (4) (9) |
| AC-18 | Wireless Access | AC-18 | | AC-18 (1) | AC-18 (1) (3) (4) (5) |
| AC-19 | Access Control for Mobile Devices | AC-19 | | AC-19 (5) | AC-19 (5) |
| AC-20 | Use of External Information Systems | AC-20 | | AC-20 (1) (2) | AC-20 (1) (2) |
| AC-21 | Information Sharing | Not Selected | | AC-21 | AC-21 |
| AC-22 | Publicly Accessible Content | AC-22 | | AC-22 | AC-22 |
| AT | Awareness and Training |  | |  |  |
| AT-1 | Security Awareness and Training Policy and Procedures | AT-1 | | AT-1 | AT-1 |
| AT-2 | Security Awareness Training | AT-2 | | AT-2 (2) | AT-2 (2) |
| AT-3 | Role-Based Security Training | AT-3 | | AT-3 | AT-3 (3) (4) |
| AT-4 | Security Training Records | AT-4 | | AT-4 | AT-4 |
| AU | Audit and Accountability |  | |  |  |
| AU-1 | Audit and Accountability Policy and Procedures | AU-1 | | AU-1 | AU-1 |
| AU-2 | Audit Events | AU-2 | | AU-2 (3) | AU-2 (3) |
| AU-3 | Content of Audit Records | AU-3 | | AU-3 (1) | AU-3 (1) (2) |
| AU-4 | Audit Storage Capacity | AU-4 | | AU-4 | AU-4 |
| AU-5 | Response to Audit Processing Failures | AU-5 | | AU-5 | AU-5 (1) (2) |
| AU-6 | Audit Review, Analysis and Reporting | AU-6 | | AU-6 (1) (3) | AU-6 (1) (3) (4) (5) (6) (7) (10) |
| AU-7 | Audit Reduction and Report Generation | Not Selected | | AU-7 (1) | AU-7 (1) |
| AU-8 | Time Stamps | AU-8 | | AU-8 (1) | AU-8 (1) |
| AU-9 | Protection of Audit Information | AU-9 | | AU-9 (2) (4) | AU-9 (2) (3) (4) |
| AU-10 | Non-repudiation | Not Selected | | Not Selected | AU-10 |
| AU-11 | Audit Record Retention | AU-11 | | AU-11 | AU-11 |
| AU-12 | Audit Generation | AU-12 | | AU-12 | AU-12 (1) (3) |
| CA | Security Assessment and Authorization | | |  |  |
| CA-1 | Security Assessment and Authorization Policies and Procedures | CA-1 | | CA-1 | CA-1 |
| CA-2 | Security Assessments | CA-2 (1) | | CA-2 (1) (2) (3) | CA-2 (1) (2) (3) |
| CA-3 | System Interconnections | CA-3 | | CA-3 (3) (5) | CA-3 (3) (5) |
| CA-5 | Plan of Action and Milestones | CA-5 | | CA-5 | CA-5 |
| CA-6 | Security Authorization | CA-6 | | CA-6 | CA-6 |
| CA-7 | Continuous Monitoring | CA-7 | | CA-7 (1) | CA-7 (1) (3) |
| CA-8 | Penetration Testing | Not Selected | | CA-8 (1) | CA-8 (1) |
| CA-9 | Internal System Connections | CA-9 | | CA-9 | CA-9 |
| CM | Configuration Management |  | |  |  |
| CM-1 | Configuration Management Policy and Procedures | CM-1 | | CM-1 | CM-1 |
| CM-2 | Baseline Configuration | CM-2 | | CM-2 (1) (2) (3) (7) | CM-2 (1) (2) (3) (7) |
| CM-3 | Configuration Change Control | Not Selected | | CM-3 (2) | CM-3 (1) (2) (4) (6) |
| CM-4 | Security Impact Analysis | CM-4 | | CM-4 | CM-4 (1) |
| CM-5 | Access Restrictions for Change | Not Selected | | CM-5 (1) (3) (5) | CM-5 (1) (2) (3) (5) |
| CM-6 | Configuration Settings | CM-6 | | CM-6 (1) | CM-6 (1) (2) |
| CM-7 | Least Functionality | CM-7 | | CM-7 (1) (2) (5)\* | CM-7 (1) (2) (5) |
| CM-8 | Information System Component Inventory | CM-8 | | CM-8 (1) (3) (5) | CM-8 (1) (2) (3) (4) (5) |
| CM-9 | Configuration Management Plan | Not Selected | | CM-9 | CM-9 |
| CM-10 | Software Usage Restrictions | CM-10 | | CM-10 (1) | CM-10 (1) |
| CM-11 | User-Installed Software | CM-11 | | CM-11 | CM-11 (1) |
| \*FedRAMP does not include CM-7 (4) in the Moderate Baseline. NIST supplemental guidance states that CM-7 (4) is not required if (5) is implemented. | | | | | |
| CP | Contingency Planning |  | |  |  |
| CP-1 | Contingency Planning Policy and Procedures | CP-1 | | CP-1 | CP-1 |
| CP-2 | Contingency Plan | CP-2 | | CP-2 (1) (2) (3) (8) | CP-2 (1) (2) (3) (4) (5) (8) |
| CP-3 | Contingency Training | CP-3 | | CP-3 | CP-3 (1) |
| CP-4 | Contingency Plan Testing | CP-4 | | CP-4 (1) | CP-4 (1) (2) |
| CP-6 | Alternate Storage Site | Not Selected | | CP-6 (1) (3) | CP-6 (1) (2) (3) |
| CP-7 | Alternate Processing Site | Not Selected | | CP-7 (1) (2) (3) | CP-7 (1) (2) (3) (4) |
| CP-8 | Telecommunications Services | Not Selected | | CP-8 (1) (2) | CP-8 (1) (2) (3) (4) |
| CP-9 | Information System Backup | CP-9 | | CP-9 (1) (3) | CP-9 (1) (2) (3) (5) |
| CP-10 | Information System Recovery and Reconstitution | CP-10 | | CP-10 (2) | CP-10 (2) (4) |
| IA | Identification and Authentication | | | | |
| IA-1 | Identification and Authentication Policy and Procedures | IA-1 | | IA-1 | IA-1 |
| IA-2 | Identification and Authentication (Organizational Users) | IA-2 (1) (12) | | IA-2 (1) (2) (3) (5) (8) (11) (12) | IA-2 (1) (2) (3) (4) (5) (8) (9) (11) (12) |
| IA-3 | Device Identification and Authentication | Not Selected | | IA-3 | IA-3 |
| IA-4 | Identifier Management | IA-4 | | IA-4 (4) | IA-4 (4) |
| IA-5 | Authenticator Management | IA-5 (1) (11) | | IA-5 (1) (2) (3) (4) (6) (7) (11) | IA-5 (1) (2) (3) (4) (6) (7) (8) (11) (13) |
| IA-6 | Authenticator Feedback | IA-6 | | IA-6 | IA-6 |
| IA-7 | Cryptographic Module Authentication | IA-7 | | IA-7 | IA-7 |
| IA-8 | Identification and Authentication (Non-Organizational Users) | IA-8 (1) (2) (3) (4) | | IA-8 (1) (2) (3) (4) | IA-8 (1) (2) (3) (4) |
| IR | Incident Response |  | |  |  |
| IR-1 | Incident Response Policy and Procedures | IR-1 | | IR-1 | IR-1 |
| IR-2 | Incident Response Training | IR-2 | | IR-2 | IR-2 (1) (2) |
| IR-3 | Incident Response Testing | Not Selected | | IR-3 (2) | IR-3 (2) |
| IR-4 | Incident Handling | IR-4 | | IR-4 (1) | IR-4 (1) (2) (3) (4) (6) (8) |
| IR-5 | Incident Monitoring | IR-5 | | IR-5 | IR-5 (1) |
| IR-6 | Incident Reporting | IR-6 | | IR-6 (1) | IR-6 (1) |
| IR-7 | Incident Response Assistance | IR-7 | | IR-7 (1) (2) | IR-7 (1) (2) |
| IR-8 | Incident Response Plan | IR-8 | | IR-8 | IR-8 |
| IR-9 | Information Spillage Response | Not Selected | | IR-9 (1) (2) (3) (4) | IR-9 (1) (2) (3) (4) |
| MA | Maintenance |  | |  |  |
| MA-1 | System Maintenance Policy and Procedures | MA-1 | | MA-1 | MA-1 |
| MA-2 | Controlled Maintenance | MA-2 | | MA-2 | MA-2 (2) |
| MA-3 | Maintenance Tools | Not Selected | | MA-3 (1) (2) (3) | MA-3 (1) (2) (3) |
| MA-4 | Nonlocal Maintenance | MA-4 | | MA-4 (2) | MA-4 (2) (3) (6) |
| MA-5 | Maintenance Personnel | MA-5 | | MA-5 (1) | MA-5 (1) |
| MA-6 | Timely Maintenance | Not Selected | | MA-6 | MA-6 |
| MP | Media Protection |  | |  |  |
| MP-1 | Media Protection Policy and Procedures | MP-1 | | MP-1 | MP-1 |
| MP-2 | Media Access | MP-2 | | MP-2 | MP-2 |
| MP-3 | Media Marking | Not Selected | | MP-3 | MP-3 |
| MP-4 | Media Storage | Not Selected | | MP-4 | MP-4 |
| MP-5 | Media Transport | Not Selected | | MP-5 (4) | MP-5 (4) |
| MP-6 | Media Sanitization | MP-6 | | MP-6 (2) | MP-6 (1) (2) (3) |
| MP-7 | Media Use | MP-7 | | MP-7 (1) | MP-7 (1) |
| PE | Physical and Environmental Protection | | |  |  |
| PE-1 | Physical and Environmental Protection Policy and Procedures | PE-1 | | PE-1 | PE-1 |
| PE-2 | Physical Access Authorizations | PE-2 | | PE-2 | PE-2 |
| PE-3 | Physical Access Control | PE-3 | | PE-3 | PE-3 (1) |
| PE-4 | Access Control for Transmission Medium | Not Selected | | PE-4 | PE-4 |
| PE-5 | Access Control for Output Devices | Not Selected | | PE-5 | PE-5 |
| PE-6 | Monitoring Physical Access | PE-6 | | PE-6 (1) | PE-6 (1) (4) |
| PE-8 | Visitor Access Records | PE-8 | | PE-8 | PE-8 (1) |
| PE-9 | Power Equipment and Cabling | Not Selected | | PE-9 | PE-9 |
| PE-10 | Emergency Shutoff | Not Selected | | PE-10 | PE-10 |
| PE-11 | Emergency Power | Not Selected | | PE-11 | PE-11 (1) |
| PE-12 | Emergency Lighting | PE-12 | | PE-12 | PE-12 |
| PE-13 | Fire Protection | PE-13 | | PE-13 (2) (3) | PE-13 (1) (2) (3) |
| PE-14 | Temperature and Humidity Controls | PE-14 | | PE-14 (2) | PE-14 (2) |
| PE-15 | Water Damage Protection | PE-15 | | PE-15 | PE-15 (1) |
| PE-16 | Delivery and Removal | PE-16 | | PE-16 | PE-16 |
| PE-17 | Alternate Work Site | Not Selected | | PE-17 | PE-17 |
| PE-18 | Location of Information System Components | Not Selected | | Not Selected | PE-18 |
| PL | Planning |  | |  |  |
| PL-1 | Security Planning Policy and Procedures | PL-1 | | PL-1 | PL-1 |
| PL-2 | System Security Plan | PL-2 | | PL-2 (3) | PL-2 (3) |
| PL-4 | Rules of Behavior | PL-4 | | PL-4 (1) | PL-4 (1) |
| PL-8 | Information Security Architecture | Not Selected | | PL-8 | PL-8 |
| PS | Personnel Security |  | |  |  |
| PS-1 | Personnel Security Policy and Procedures | PS-1 | | PS-1 | PS-1 |
| PS-2 | Position Risk Designation | PS-2 | | PS-2 | PS-2 |
| PS-3 | Personnel Screening | PS-3 | | PS-3 (3) | PS-3 (3) |
| PS-4 | Personnel Termination | PS-4 | | PS-4 | PS-4 (2) |
| PS-5 | Personnel Transfer | PS-5 | | PS-5 | PS-5 |
| PS-6 | Access Agreements | PS-6 | | PS-6 | PS-6 |
| PS-7 | Third-Party Personnel Security | PS-7 | | PS-7 | PS-7 |
| PS-8 | Personnel Sanctions | PS-8 | | PS-8 | PS-8 |
| RA | Risk Assessment |  | |  |  |
| RA-1 | Risk Assessment Policy and Procedures | RA-1 | | RA-1 | RA-1 |
| RA-2 | Security Categorization | RA-2 | | RA-2 | RA-2 |
| RA-3 | Risk Assessment | RA-3 | | RA-3 | RA-3 |
| RA-5 | Vulnerability Scanning | RA-5 | | RA-5 (1) (2) (3) (5) (6) (8) | RA-5 (1) (2) (3) (4) (5) (6) (8) (10) |
| SA | System and Services Acquisition |  | |  |  |
| SA-1 | System and Services Acquisition Policy and Procedures | SA-1 | | SA-1 | SA-1 |
| SA-2 | Allocation of Resources | SA-2 | | SA-2 | SA-2 |
| SA-3 | System Development Life Cycle | SA-3 | | SA-3 | SA-3 |
| SA-4 | Acquisition Process | SA-4 (10) | | SA-4 (1) (2) (8) (9) (10) | SA-4 (1) (2) (8) (9) (10) |
| SA-5 | Information System Documentation | SA-5 | | SA-5 | SA-5 |
| SA-8 | Security Engineering Principles | Not Selected | | SA-8 | SA-8 |
| SA-9 | External Information System Services | SA-9 | | SA-9 (1) (2) (4) (5) | SA-9 (1) (2) (4) (5) |
| SA-10 | Developer Configuration Management | Not Selected | | SA-10 (1) | SA-10 (1) |
| SA-11 | Developer Security Testing and Evaluation | Not Selected | | SA-11 (1) (2) (8) | SA-11 (1) (2) (8) |
| SA-12 | Supply Chain Protection | Not Selected | | Not Selected | SA-12 |
| SA-15 | Development Process, Standards and Tools | Not Selected | | Not Selected | SA-15 |
| SA-16 | Developer-Provided Training | Not Selected | | Not Selected | SA-16 |
| SA-17 | Developer Security Architecture and Design | Not Selected | | Not Selected | SA-17 |
| SC | System and Communications Protection | | |  |  |
| SC-1 | System and Communications Protection Policy and Procedures | | SC-1 | SC-1 | SC-1 |
| SC-2 | Application Partitioning | | Not Selected | SC-2 | SC-2 |
| SC-3 | Security Function Isolation | | Not Selected | Not Selected | SC-3 |
| SC-4 | Information in Shared Resources | | Not Selected | SC-4 | SC-4 |
| SC-5 | Denial of Service Protection | | SC-5 | SC-5 | SC-5 |
| SC-6 | Resource Availability | | Not Selected | SC-6 | SC-6 |
| SC-7 | Boundary Protection | | SC-7 | SC-7 (3) (4) (5) (7) (8) (12) (13) (18) | SC-7 (3) (4) (5) (7) (8) (10) (12) (13) (18) (20) (21) |
| SC-8 | Transmission Confidentiality and Integrity | | Not Selected | SC-8 (1) | SC-8 (1) |
| SC-10 | Network Disconnect | | Not Selected | SC-10 | SC-10 |
| SC-12 | Cryptographic Key Establishment and Management | | SC-12 | SC-12 (2) (3) | SC-12 (1) (2) (3) |
| SC-13 | Cryptographic Protection | | SC-13 | SC-13 | SC-13 |
| SC-15 | Collaborative Computing Devices | | SC-15 | SC-15 | SC-15 |
| SC-17 | Public Key Infrastructure Certificates | | Not Selected | SC-17 | SC-17 |
| SC-18 | Mobile Code | | Not Selected | SC-18 | SC-18 |
| SC-19 | Voice Over Internet Protocol | | Not Selected | SC-19 | SC-19 |
| SC-20 | Secure Name / Address Resolution Service (Authoritative Source) | | SC-20 | SC-20 | SC-20 |
| SC-21 | Secure Name / Address Resolution Service (Recursive or Caching Resolver) | | SC-21 | SC-21 | SC-21 |
| SC-22 | Architecture and Provisioning for Name / Address Resolution Service | | SC-22 | SC-22 | SC-22 |
| SC-23 | Session Authenticity | | Not Selected | SC-23 | SC-23 (1) |
| SC-24 | Fail in Known State | | Not Selected | Not Selected | SC-24 |
| SC-28 | Protection of Information at Rest | | Not Selected | SC-28 (1) | SC-28 (1) |
| SC-39 | Process Isolation | | SC-39 | SC-39 | SC-39 |
| SI | System and Information Integrity | | | | |
| SI-1 | System and Information Integrity Policy and Procedures | | SI-1 | SI-1 | SI-1 |
| SI-2 | Flaw Remediation | | SI-2 | SI-2 (2) (3) | SI-2 (1) (2) (3) |
| SI-3 | Malicious Code Protection | | SI-3 | SI-3 (1) (2) (7) | SI-3 (1) (2) (7) |
| SI-4 | Information System Monitoring | | SI-4 | SI-4 (1) (2) (4) (5) (14) (16) (23) | SI-4 (1) (2) (4) (5) (11) (14) (16) (18) (19) (20) (22) (23) (24) |
| SI-5 | Security Alerts, Advisories and Directives | | SI-5 | SI-5 | SI-5 (1) |
| SI-6 | Security Function Verification | | Not Selected | SI-6 | SI-6 |
| SI-7 | Software, Firmware and Information Integrity | | Not Selected | SI-7 (1) (7) | SI-7 (1) (2) (5) (7) (14) |
| SI-8 | Spam Protection | | Not Selected | SI-8 (1) (2) | SI-8 (1) (2) |
| SI-10 | Information Input Validation | | Not Selected | SI-10 | SI-10 |
| SI-11 | Error Handling | | Not Selected | SI-11 | SI-11 |
| SI-12 | Information Handling and Retention | | SI-12 | SI-12 | SI-12 |
| SI-16 | Memory Protection | | SI-16 | SI-16 | SI-16 |

Note that “-1” Controls (AC-1, AU-1, SC-1, etc.) \* cannot be inherited and must be described in some way by the service provider.  
\*Access Control (AC), Audit and Accountability (AU), System and Communications Protection (SC)

The definitions in Table 13‑2 Control Origination and Definitions indicate where each security control originates.

Table 13‑2 Control Origination and Definitions

| Control Origination | Definition | Example |
| --- | --- | --- |
| Service Provider Corporate | A control that originates from the Microsoft Corporation 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 system at the Microsoft Corporation 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 system at the Microsoft Corporation. | There are scans of the corporate network infrastructure; scans of databases and web based application are system specific. |
| Configured by Customer | A control where the customer needs to apply a configuration in order 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 the customer needs to provide additional hardware or software in order to meet the control requirement. | The customer provides a SAML SSO solution to implement two-factor authentication. |
| Shared | A control that is managed and implemented partially by the Microsoft Corporation and partially by the customer. | Security awareness training must be conducted by both the CSPN and the customer. |
| Inherited from pre-existing FedRAMP Authorization | A control that is inherited from another Microsoft Corporation system that has already received a FedRAMP Authorization. | A PaaS or SaaS provider inherits PE controls from an IaaS provider. |

* 1. Access Control (AC)

### AC-1 Access Control Policy and Procedures Requirements (L) (M)

The organization:

1. Develops, documents and disseminates to [Assignment: organization-defined personnel or roles]:

An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

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

Reviews and updates the current:

Access control policy [FedRAMP Assignment: at least every 3 years]; and

Access control procedures [FedRAMP Assignment: at least annually].

| AC-01 | Control Summary Information |
| --- | --- |
| Responsible Role: Customer Administrator, Office 365 Trust Program Manager, Program Manager | |
| Parameter AC-01(a)(1):  Service Engineer Operations, Program Manager, Developer, Tester, Office 365 Trust Program Manager, Office 365 Security Manager, BCM | |
| Parameter AC-01(a)(2):  Service Engineer Operations, Program Manager, Developer, Tester, Office 365 Trust Program Manager, Office 365 Security Manager, BCM | |
| Parameter AC-01(b)(1):  Annually | |
| Parameter AC-01(b)(2):  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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869) | |

| AC-01 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility:**  Government customers are responsible for developing and maintaining appropriate Access Control policies and procedures that govern access management activities for their organization and users.  **Part 1:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Information Security Policy defines Office 365 MT policies. This document addresses the purpose, scope, roles, responsibilities, compliance requirements, and required coordination among the various Microsoft organizations providing some level of support for the security of Office 365 MT. Policies are distributed via SharePoint to personnel responsible for implementing access control policies and procedures.  **Part 2:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Standards and procedures to facilitate execution of the Office 365 Information Security Policy are documented in the Active Framework Controls, Office 365 Standard Operating Procedures (SOPs), and service team-specific SOPs. These standards and procedures act as adjuncts to the security policy and provide implementation level requirements and details to carry out specific operational tasks. Office 365 SOPs are distributed via SharePoint to roles providing support for Office 365 MT security. |
| Part b | **Customer Responsibility:**  Government customers are responsible for annually updating their Access Control policies and procedures.  **Part 1:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Information Security Policy is reviewed and updated annually by the Office 365 Trust team.  **Part 2:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 SOPs are reviewed and updated annually. |

### AC-2 Account Management (L) (M)

The organization:

1. Identifies and selects the following types of information system accounts to support organizational missions/business functions: [Assignment: organization-defined information system account types];
2. Assigns account managers for information system accounts;
3. Establishes conditions for group and role membership;
4. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
5. Requires approvals by [Assignment: organization-defined personnel or roles] for requests to create information system accounts;
6. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions];
7. Monitors the use of information system accounts;
8. Notifies account managers:
   1. When accounts are no longer required;
   2. When users are terminated or transferred; and
   3. When individual information system usage or need-to-know changes;
9. Authorizes access to the information system based on:
   1. A valid access authorization;
   2. Intended system usage; and
   3. Other attributes as required by the organization or associated missions/business functions;
10. Reviews accounts for compliance with account management requirements [FedRAMP Assignment: at least annually]; and
11. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

| AC-02 | Control Summary Information |
| --- | --- |
| Responsible Role: Customer Administrator, Office 365 Trust Program Manager, Program Manager | |
| Parameter AC-02(a):  Service Team, Customer, and Service Accounts | |
| Parameter AC-02(e):  account managers identified in Microsoft account management tools | |
| Parameter AC-02(f):  Microsoft Office 365 Security Policy | |
| Parameter AC-02(j):  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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869) | |

| AC-02 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility:**  All customers, including government and non-government customers, are responsible for identifying the account types for their organization in compliance with their organizational policies. Government and non-government customers using ADFS will configure their account types in their existing Active Directory infrastructure. Non-government customers not using ADFS will configure account types in AAD via SUE.  For more information on managing customer account types via the SUE portal, see the following link: http://technet.microsoft.com/en-us/library/office-365-user-account-management.aspx  Guest access to SFB meetings, if enabled, allows anyone with a meeting invite to access the meeting lobby; this method of guest access is considered session access as no account is assigned to the guest user. The meeting organizer is responsible for establishing the identity of lobby participants before granting them access to the meeting. Government customers are responsible for disabling guest access to SFB meetings to remain compliant with FedRAMP standards as advised in "Office 365 MT Government Compliance Considerations v 2 00".  Non-government customers are responsible for determining if the use of guest access to SFB meetings should be allowed for their organization. This setting can be configured by government and non-government customers. For more information, see the following TechNet article: http://technet.microsoft.com/en-US/library/gg398648.aspx  SharePoint Online guest invitations allow external users to access an organization’s SharePoint Online site(s). Government and non-government customers are responsible for determining if the use of guest access to SharePoint Online, as an account type, should be allowed for their organization. Government customers are responsible for disabling guest access to SharePoint Online to remain compliant with FedRAMP standards as advised in "Office 365 MT Government Compliance Considerations ". The setting to allow or disallow guest access to SharePoint Online can be configured by government and non-government customers.  For more information, see the following Office 365 MT help article: http://office.microsoft.com/en-us/office365-sharepoint-online-small-business-help/manage-sharing-with-external-users-HA102849862.aspx  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT has identified and selected three categories of accounts within Office 365 MT to support organizational missions/business functions: service team, customer, and service.  Service team accounts are used individually by service team personnel to manage and administer Office 365 MT. Service teams divide the service team account type into separate roles as required to meet separation of duties requirements.  Customer accounts are used by customer users to access the Office 365 MT product. Customer accounts are managed by the customer.  Service accounts are used by Office 365 MT service team services to authenticate to servers and other services. |
| Part b | **Customer Responsibility:**  All customers, including government and non-government customers, are responsible for assigning account managers for the account types identified in part a of this control.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT assigns account managers to each role type using account management tools such as IDM, OneIdentity, IDWeb, and RAMWeb. Throughout this SSP these tools are collectively referenced as "account management tools". |
| Part c | **Customer Responsibility:**  All customers, including government and non-government customers, are responsible for establishing conditions for group/role membership for their organization in compliance with their organizational policies. Government and non-government customers using ADFS will configure their groups/roles in their existing Active Directory infrastructure. Non-government customers not using ADFS will configure groups in AAD via SUE.  For more information on managing customer groups/roles in AAD via the SUE portal, see the following link: http://technet.microsoft.com/en-us/library/office-365-user-account-management.aspx  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Service teams establish conditions for group/role membership by defining and enforcing conditions for each group/role in account management tools. In addition, service teams use JIT Tools to enforce additional, more granular conditions for privilege escalation and approval for interactive sessions.  Office 365 MT establishes conditions for group and role membership based on least privilege necessary for a user to perform their assigned duties. Predetermined conditions are established when groups are created. |
| Part d | **Customer Responsibility:**  Government and non-government customers using ADFS are responsible for identifying organizationally authorized users and specifying access privileges for those users using their existing Active Directory (AD) infrastructure. These 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's ADFS server then communicates that identification/authentication and the associated permissions to AAD via SAML2.0 ticket.  For more information on managing user accounts in Active Directory, see TechNet article #754661: http://technet.microsoft.com/en-us/library/cc754661.aspx  Non-government customers not using ADFS will manage user accounts in AAD via SUE. For these customers, AAD is responsible for identifying organizationally authorized users and will enforce the access privileges defined by the customer.  For more information on managing customer user identifiers and specifying access privileges in AAD via the SUE portal, see the following link: http://technet.microsoft.com/en-us/library/office-365-user-account-management.aspx  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Role Based Access Control (RBAC) is used to identify and control the access privileges of each service team personnel. Access privileges vary depending on the role that a specified service team personnel will assume within the service team. Access privileges are defined in account management tools and enforced by Active Directory. In addition, service teams use JIT Tools to enforce additional, more granular conditions for privilege escalation and approval for interactive sessions.  By default, these service team accounts initially belong to a security group that has remote system metadata read access, and no direct access to the production environment. If service team personnel need additional access to the production environment, they request that access and provide business justification using Just-In-Time (JIT) tools. Service team personnel with the access approver role then review and approve or deny the type of access requested. Access is only provided for a finite period of time based on the expected duration of the work to be performed. If access is approved, JIT tools assign the service team personnel to security groups with the minimum permissions required to perform the work and automatically revokes permissions at the end of the specified time period. |
| Part e | **Customer Responsibility:**  All customers, including government and non-government customers, are responsible for requiring appropriate approvals for requests to establish organizational accounts in compliance with their organizational policies. Government and non-government customers using ADFS will manage their accounts in their existing Active Directory infrastructure. Non-government customers not using ADFS will manage their accounts in AAD via SUE.  For more information on managing customer accounts via the SUE portal, see the following link: http://technet.microsoft.com/en-us/library/office-365-user-account-management.aspx  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  In order to gain access to the Office 365 MT production environment, service team personnel must first request access via the account management tools; access to the production environment is provided via security group membership. Approval to establish the account from the service team’s management is required for a service team administrator to be added to the appropriate security group. These approvals are tracked and enforced by account management tools.  Additionally, access to DNS is provided through PHX security group membership, which is managed and maintained through the Microsoft account management tool OneIdentity. Approval to establish accounts is required from the DNS service team management and the DNS service team operations leads, as well as to obtain membership to the appropriate security group within PHX. These approvals are tracked and enforced by OneIdentity. |
| Part f | **Customer Responsibility:**  Government customers are responsible for establishing, activating, modifying, disabling, and removing organizational accounts in accordance with their procedures using their Active Directory (AD) infrastructure. Government users authenticate to government-owned ADFS servers which utilize the government AD infrastructure to identify, authenticate, and apply permissions to that user's session. The government ADFS server then communicates that identification/authentication, and the associated permissions to AAD via SAML2.0 ticket.  For more information on managing user accounts in Active Directory, see TechNet article #754661: http://technet.microsoft.com/en-us/library/cc754661.aspx  Non-government customers using ADFS establish, activate, modify, disable, and remove organizational accounts following the same procedures outlined for government customers. Non-government customers not using ADFS manage user accounts in AAD via SUE.  For more information on managing customer accounts via the SUE portal, see the following link: http://technet.microsoft.com/en-us/library/office-365-user-account-management.aspx  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Account changes are managed through account management tools in accordance with the Office 365 Information Security Policy and rules which have been defined in account management tools. |
| Part g | **Customer Responsibility:**  Government and non-government customers using ADFS are responsible for monitoring the use of information system accounts managed by their Active Directory. See AU-2, AU-3, AU-6, and SI-4 for more details about these responsibilities.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT monitors the use of information system accounts in accordance with the AU family of security controls. Office 365 MT records the auditable events defined in AU-2 with the content defined in AU-3 and monitors those records in accordance with the control descriptions for AU-6 and SI-4. |
| Part h | **Customer Responsibility:**  Government and non-government customers are responsible for implementing processes to notify customer account managers when accounts are no longer required, when users are terminated or transferred, or when individual information system usage or need-to-know changes.  **Part 1,2,3:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT Service teams have automated workflow account management tools that allow the service teams to track the account management process through account request, approval, creation, modification, and deletion. As changes occur, the corresponding account manager is notified of the changes that require their approval. Information system usage and need-to-know are mapped to the roles defined by each service team. When an employee is transferred or their employment is terminated, the account management tools will automatically revoke the associated account's access to the privileges mapped to their previous role. |
| Part i | **Customer Responsibility:**  Government customers are responsible for managing organizational user accounts by granting access to Office 365 MT based on: a valid access authorization; intended system usage; and other attributes as required by the organization or associated missions/business functions using their Active Directory (AD) infrastructure. Government users authenticate to government owned ADFS servers which utilize the government AD infrastructure to identify, authenticate, and apply permissions to that user’s session. The government ADFS server then communicates that identification/authentication, and the associated permissions to AAD via SAML2.0 ticket.  For more information on managing user accounts in Active Directory, see TechNet article #754661: http://technet.microsoft.com/en-us/library/cc754661.aspx  Non-government customers can manage organizational user accounts by granting access to Office 365 MT based on: a valid access authorization; intended system usage; and other attributes as required by the organization or associated missions/business functions following the same procedures outlined for government customers, or they can elect to manage user accounts in AAD via SUE.  For more information on managing customer accounts via the SUE portal, see the following link: http://technet.microsoft.com/en-us/library/office-365-user-account-management.aspx  **Part 1,2,3:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Membership in security groups that give access to the system is given only to those in specific roles that require system access. Service team managers are responsible for approving group membership. The managers validate that the user requires access to the production environment to fulfill their duties and support Office 365 MT. Access is granted based on this valid access authorization and documented intended systems usage consistent with the permission type and conditions for group membership.  In addition, some teams use JIT tools to enforce additional, more granular conditions. If intended system usage requires approval additional approval must be granted to gain access. The On-Call approver is responsible for validating that the requested just in time permissions are required to support the mission/business functions of Office 365 MT. |
| Part j | Customer Responsibility:  Office 365 MT Customers are responsible for reviewing the accounts of their organization’s users in compliance with their organizational policies. Office 365 MT allows two methods for customers to manage/review their user accounts: ADFS and SUE.  ADFS: Government and non-government customers using ADFS manage user accounts in their own customer-owned and controlled Active Directory (AD) forests. These customers should review their AD accounts as required by their internal policies (at least annually to comply with FedRAMP requirements). If customers disable or remove users in their Active Directory during this review, those users will immediately no longer have access to Office 365 MT.  For more information on managing user accounts in Active Directory, see TechNet article #754661: http://technet.microsoft.com/en-us/library/cc754661.aspx  SUE: Non-government customers not using ADFS may manage accounts in Azure Active Directory via the Suite User Experience (SUE) portal. Customers are responsible for logging into the portal and reviewing the Office 365 MT accounts of their users compliant with their organizational policies. Disabling or removing users in the SUE portal revokes access to Office 365 MT for the affected users.  For more information on managing user accounts via the SUE portal, see TechNet article “office 365 user account management”: http://technet.microsoft.com/en-us/library/office-365-user-account-management.aspx  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 MT service teams review service team administrator accounts at least quarterly. |
| Part k | **Customer Responsibility:**  If government or non-government customers allow the use of shared customer accounts, they are responsible for reissuing shared account credentials when individuals are removed from or leave the group. Government and non-government customers using ADFS will reissue credentials using their ADFS infrastructure. Non-government customers not using ADFS will reissue credentials in AAD via SUE.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT does not allow the use of shared/group user accounts. Individual service engineers are assigned into a security group, and in order to use these credentials, a user must go through multifactor authentication to uniquely identify their credentials. |

#### AC-2 (1) Control Enhancement (M) (H)

The organization employs automated mechanisms to support the management of information system accounts.

| AC-02(1) | Control Summary Information |
| --- | --- |
| Responsible Role: Customer Administrator, Office 365 Security Manager, Office 365 Trust Program Manager, Program Manager | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AC-02(1) - What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility:**  Government customers using ADFS are responsible for employing their Active Directory (AD) infrastructure as automated mechanisms to support their organizational user accounts. Government users authenticate to government owned ADFS servers which utilize the government AD infrastructure to automatically identify, authenticate, and apply permissions to that user’s session. The government ADFS server then communicates that identification/authentication, and the associated permissions to AAD via SAML2.0 ticket.  For more information on managing user accounts in Active Directory, see TechNet article #754661: http://technet.microsoft.com/en-us/library/cc754661.aspx.  Non-government customers can employ AD as an automated mechanism following the same procedures outlined for government customers, or they can elect to manage user accounts in AAD via SUE. For customers not using ADFS, AAD is employed as an automated mechanism to support their organizational user accounts.  For more information on managing customer accounts via the SUE portal, see the following link: http://technet.microsoft.com/en-us/library/office-365-user-account-management.aspx.  **DNS:**  The Microsoft account management tool OneIdentity is used for automated user and service account management of Global Management Environment (GME) accounts.  **Bing, Delve, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  IDM is an automated workflow management tool that allows service teams to manage service team administrator and service accounts through account request, approval, creation, modification, and deletion. IDM integrates with Microsoft Online Directory Service (MSODS) to provide identity synchronization, certificate management, service team administrator password resets and service team administrator provisioning from a single interface. Service team managers are responsible for approving requests in IDM.  By default, service team Active Directory accounts belong to a security group that only has read access to the production environment. Additionally, if a service team administrator needs elevated privileges to the production environment, they request that access, providing a business justification using JIT tools. A service team administrator with the access approver role then reviews and approves or denies the type of access requested. Access is only provided for a finite period of time based on the expected duration of the work to be performed. If access is approved, JIT tools assign the service team administrator to security groups with the minimum permissions required to perform the work and automatically revokes permissions at the end of the specified time period.  Bing and SFB also use RAMWeb to manage security groups, which are used to gain access to Azure PaaS services, Source Depot, and configuration files. |

#### AC-2 (2) Control Enhancement (M)

The information system automatically [Selection: removes; disables] temporary and emergency accounts after [FedRAMP Assignment: no more than 30 days for temporary and emergency account types].

| AC-02(2) | Control Summary Information |
| --- | --- |
| Responsible Role: Customer Administrator, None – Not Applicable | |
| Parameter AC-02(2):  1. disables; 2. no more than 30 days for temporary and emergency account types | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AC-02(2) - What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility:**  Government customers are responsible for automatically terminating temporary and emergency government customer accounts, in compliance with their organizational policies, using their Active Directory (AD) infrastructure (no more than 90 days for FedRAMP compliance). Government users authenticate to government managed ADFS servers which utilize the government AD infrastructure to identify, authenticate, and apply permissions to that user’s session. The government ADFS server then communicates that identification/authentication and the associated permissions to AAD via SAML2.0 ticket.  For more information on managing user accounts in Active Directory, see TechNet article #754661: http://technet.microsoft.com/en-us/library/cc754661.aspx  Non-government customers can manage terminating temporary and emergency accounts following the same procedures outlined for government customers, or they can elect to manage user accounts in AAD via SUE. For customers using AAD the process for terminating temporary and emergency accounts will be manual.  For more information on managing accounts via the SUE portal, see the following link: http://technet.microsoft.com/en-us/library/office-365-user-account-management.aspx  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT prohibits the use of temporary and emergency accounts. All local guest accounts are disabled by service team engineers. All account requests go through the standard account management processes. |

#### AC-2 (3) Control Enhancement (M)

The information system automatically disables inactive accounts after [FedRAMP Assignment: ninety (90) days for user accounts].

AC-2 (3) Additional FedRAMP 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 Joint Authorization Board (JAB)/AO. Where user management is a function of the service, reports of activity of consumer users shall be made available.

| AC-02(3) | Control Summary Information |
| --- | --- |
| Responsible Role: Customer Administrator, Office 365 Security Manager, Office 365 Trust Program Manager, Service Engineer Operations | |
| Parameter AC-02(3):  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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AC-02(3) - What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility:**  Government customers are responsible for automatically disabling inactive government customer accounts, in compliance with their organizational policies, using their Active Directory (AD) infrastructure (no more than 90 days for FedRAMP compliance). Government users authenticate to government owned ADFS servers which utilize the government AD infrastructure to identify, authenticate, and apply permissions to that user’s session. The government ADFS server then communicates that identification/authentication and the associated permissions to AAD via SAML2.0 ticket.  For more information on managing user accounts in Active Directory, see TechNet article #754661: http://technet.microsoft.com/en-us/library/cc754661.aspx  Non-government customers can manage disabling inactive accounts following the same procedures outlined for government customers, or they can elect to manage user accounts in AAD via SUE. For customers using AAD, the process for disabling inactive accounts will be manual.  For more information on disabling inactive accounts via the SUE portal, see the following link: http://technet.microsoft.com/en-us/library/office-365-user-account-management.aspx  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Inactive accounts are disabled after no more than 90 days. |

#### AC-2 (4) Control Enhancement (M)

The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies [Assignment: organization-defined personnel or roles].

| AC-02(4) | Control Summary Information |
| --- | --- |
| Responsible Role: Customer Administrator, Office 365 Trust Program Manager, Service Engineer Operations | |
| Parameter AC-02(4):  account manager defined in Microsoft account management tools, Office 365 Security Analysis & Response (Office 365 Security A&R) | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AC-02(4) - What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility:**  Government customers are responsible for automatically auditing account creation, modification, disabling, and termination actions as well as notifying appropriate individuals for change to their organizational user accounts, in compliance with their organizational policies, using their Active Directory (AD) infrastructure. Government users authenticate to government owned ADFS servers which utilize the government AD infrastructure to identify, authenticate, and apply permissions to that user’s session. The government ADFS server then communicates that identification/authentication and the associated permissions to AAD via SAML2.0 ticket.  For more information on managing user accounts in Active Directory, see TechNet article #754661: http://technet.microsoft.com/en-us/library/cc754661.aspx  Non-government customers can audit account creation, modification, disabling, and termination actions as well as notify appropriate individuals for change to their organizational user accounts following the same procedures outlined for government customers, or they can elect to manage user accounts in AAD via SUE. For customers using AAD, audit records of account creation, modification, disabling, and termination will be retained for 90 days; the process for notifying appropriate individuals for change to their organizational user accounts will be manual.  For more information on managing customer accounts via the SUE portal, see the following link: http://technet.microsoft.com/en-us/library/office-365-user-account-management.aspx  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT performs automated auditing of privileged service team accounts through Microsoft account management tools, which provide a record of account creation, modification, disabling, and termination of accounts. A notification is sent to the account manager when accounts are changed or managed in any way. |

#### AC-2 (5) Control Enhancement (M)

The organization requires that users log out when [Assignment: organization-defined time-period of expected inactivity or description of when to log out].

AC-2 (5) Additional FedRAMP Requirements and Guidance:

Guidance: Should use a shorter timeframe than AC-12

| AC-02(5) | Control Summary Information |
| --- | --- |
| Responsible Role: Customer Administrator, Office 365 Trust Program Manager, Service Engineer Operations | |
| Parameter AC-02(5):  any expected unattended inactivity or when the task that was the purpose of the log on is complete | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AC-02(5) - What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility:**  Government and non-government customers are responsible for identifying and implementing their own requirements for expected inactivity or description of when to log out for their customers.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT requires that service team administrators log out of Office 365 MT in advance of any expected unattended inactivity, or when they have completed the task that was the purpose of the log in. |

#### AC-2 (7) Control Enhancement (M)

The organization:

1. Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles;
2. Monitors privileged role assignments; and
3. Takes [Assignment: organization-defined actions] when privileged role assignments are no longer appropriate.

| AC-02(7) | Control Summary Information |
| --- | --- |
| Responsible Role: Customer Administrator, Office 365 Security Manager, Office 365 Trust Program Manager | |
| Parameter AC-02(7)(c):  actions to disable 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AC-02(7) - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility:**  All customers, including government and non-government customers, are responsible for establishing and administering privileged user accounts with a role-based access scheme that organizes Office 365 MT customer privileges into roles in compliance with their organizational policies.  Government and non-government customers using ADFS will manage their account roles in their existing Active Directory infrastructure. For more information on managing user accounts in Active Directory, see TechNet article #754661: http://technet.microsoft.com/en-us/library/cc754661.aspx  Non-government customers not using ADFS will manage their account roles in AAD via SUE. For more information on managing customer accounts via the SUE portal, see the following link: http://technet.microsoft.com/en-us/library/office-365-user-account-management.aspx  **DNS, OSI, SFB, SWE:**  All service team personnel accounts are considered privileged. Service team personnel are assigned a role within their service team that corresponds to a security group. Each security group is assigned permissions to correlating environments with just enough access to properly fulfill their tasks. Service team managers are responsible for approving role assignments.  **Bing, Delve, EXO, IP, MSTeams, OLM, SPO, SUE, WAC:**  All service team personnel accounts are considered privileged. Service team users are assigned to security roles, which have a defined list of available permissions. By default, service team accounts belong to a security group that only has remote access to read system metadata, and no direct access to the production environment. If a service team user needs elevated privileges to the production environment, they must request that access and provide a business justification using Just-In-Time (JIT) tools. A service team user with the access approver role then reviews and approves or denies the type of access requested. Access is only provided for a finite period of time based on the expected duration of the work to be performed. If access is approved, JIT tools assign the service team user to security groups with the minimum permissions required to perform the work and automatically revoke permissions at the end of the specified time period. |
| Part b | **Customer Responsibility:**  Government customers are responsible for tracking and monitoring privileged role assignments, in compliance with their organizational policies, using their Active Directory (AD) infrastructure. Government users authenticate to government owned ADFS servers which utilize the government AD infrastructure to identify, authenticate, and apply permissions to that user’s session. The government ADFS server then communicates that identification/authentication and the associated permissions to AAD via SAML2.0 ticket.  For more information on managing user accounts in Active Directory, see TechNet article #754661: http://technet.microsoft.com/en-us/library/cc754661.aspx  Non-government customers can track and monitor privileged role assignments following the same procedures outlined for government customers, or they can elect to manage user accounts in AAD via SUE. For customers using AAD, audit records of assignment to privileged roles will be retained for 90 days; the process for tracking privileged role assignments will be manual.  For more information on managing customer account role assignments via the SUE portal, see the following link: http://technet.microsoft.com/en-us/library/office-365-user-account-management.aspx  **DNS, OSI, SFB, SWE:**  All service team accounts are considered privileged, and are tracked and monitored using automated account management tools.  **Bing, Delve, EXO, IP, MSTeams, OLM, SPO, SUE, WAC:**  All service team accounts are considered privileged, and are tracked and monitored using automated account management tools. If a service team user needs additional elevated access to the production environment they must request that access and provide a business justification using JIT tools, which track and monitor the role assignment. |
| Part c | **Customer Responsibility:**  Government and non-government customers are responsible for defining and taking required actions when privileged role assignments for customer users are no longer appropriate.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Privileged role assignments are no longer appropriate when Office 365 MT personnel no longer have need of the role to support their current work, or if their employment with Microsoft is terminated. In those cases, Office 365 MT follows account management workflows to disable the account or revoke access. |

#### AC-2 (9) Control Enhancement (M)

The organization only permits the use of shared/group accounts that meet [Assignment: organization-defined conditions for establishing shared/group accounts].

AC-2 (9) Additional FedRAMP Requirements and Guidance: Required if shared/group accounts are deployed.

| AC-02(9) | Control Summary Information |
| --- | --- |
| Responsible Role: Customer Administrator, Office 365 Security Manager, Office 365 Trust Program Manager | |
| Parameter AC-02(9):  the condition of users gaining access via a shared/group account being linked to an individual user 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AC-02(9) - What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility:**  Government and non-government customers are responsible for defining conditions for establishing shared/group accounts and enforcing those conditions if they choose to establish shared/group accounts.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT does not allow the use of shared/group user accounts. |

#### AC-2 (10) Control Enhancement (M) (H)

The information system terminates shared/group account credentials when members leave the group.

AC-2 (10) Additional FedRAMP Requirements and Guidance: Required if shared/group accounts are deployed.

| AC-02(10) | Control Summary Information |
| --- | --- |
| Responsible Role: Customer Administrator, Office 365 Security Manager, Office 365 Trust Program Manager | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AC-02(10) - What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility:**  If government or non-government customers allow the use of group shared customer accounts, they are responsible for terminating group/shared account credentials when individuals leave the group. Government and non-government customers using ADFS will terminate credentials using their ADFS infrastructure. Non-government customers not using ADFS will terminate credentials using SUE.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT does not allow the use of shared/group user accounts. |

#### AC-2 (12) Control Enhancement (M)

The organization:

1. Monitors information system accounts for [Assignment: organization-defined atypical use]; and
2. Reports atypical usage of information system accounts to [Assignment: organization-defined personnel or roles].

AC-2 (12) (a) and AC-2 (12) (b) Additional FedRAMP Requirements and Guidance: Required for privileged accounts.

| AC-02(12) | Control Summary Information |
| --- | --- |
| Responsible Role: Customer Administrator, Office 365 Security Manager, Office 365 Trust Program Manager | |
| Parameter AC-02(12)(a):  atypical use configured in NRT Security Monitoring and automated security alerting tools alert logic | |
| Parameter AC-02(12)(b):  Office 365 Security Incident Response (Office 365 SIR) | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AC-02(12) - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility:**  Government and non-government customers using ADFS are responsible for defining atypical use and monitoring for that use on their ADFS infrastructure. Government and non-government customers can additionally review Office 365 MT application logs and analyze them for atypical use.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT monitors for atypical use by monitoring for indications of compromise - using near real time (NRT) monitoring and automated security alerting tools - as directed by the Office 365 Security team. |
| Part b | **Customer Responsibility:**  Government and non-government customers are responsible for reporting atypical usage to defined organizational personnel.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT follows normal incident reporting procedures if atypical usage is detected. These procedures require reporting incidents to the Office 365 Security Incident Response (SIR) team. |

### AC-3 Access Enforcement (L) (M) (H)

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

| AC-03 | Control Summary Information |
| --- | --- |
| Responsible Role: Customer Administrator, Office 365 Security Manager, Office 365 Trust Program Manager, 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AC-03 - What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility:**  Government customers are responsible for enforcing approved authorizations for logical access to the system, in compliance with their organizational policies, using their Active Directory (AD) infrastructure. Government users authenticate to government owned ADFS servers which utilize the government AD infrastructure to identify, authenticate, and apply permissions to that user’s session. The government ADFS server then communicates that identification/authentication and the associated permissions to AAD via SAML2.0 ticket. Once permissions are communicated to AAD, AAD is responsible for enforcing those permissions for the user’s Office 365 MT session.  For more information on managing user accounts in Active Directory, see TechNet article #754661: http://technet.microsoft.com/en-us/library/cc754661.aspx  Non-government customers can enforce approved authorizations for logical access to the system following the same procedures outlined for government customers, or they can elect to manage user accounts in AAD via SUE. For customers using AAD, AAD is responsible for enforcing the approved authorizations set by the customer in the SUE portal.  For more information on managing customer account privileges via the SUE portal, see the following link: http://technet.microsoft.com/en-us/library/office-365-user-account-management.aspx  **DNS:**  The DNS service team enforces approved authorizations for logical access using role-based access control enforced by Active Directory. The Office 365 DNS service team's servers are located within the Azure maintained PHX domain. Access to the DNS service team's equipment is restricted to the specifically authorized security group within the PHX domain. The DNS service team operations personnel maintain membership to this security group through the account management tool OneIdentity. All requests to be added to the security group must be specifically approved by the DNS service team operations leads or management.  **Bing, Delve, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 service teams enforce approved authorizations for logical access using role-based access control enforced by Active Directory (AD) and Azure Active Directory (AAD). Office 365 MT uses AD to implement role-based access control (RBAC) via the use of AD groups. For the purposes of this control, the term "security group" references an AD group which is used to enforce RBAC permissions.  Service teams are responsible for managing security groups in the production domain. Office 365 MT has three major account types: service team, customer, and service. Service team accounts are used by service team personnel to manage and administer Office 365 MT. Customer accounts are used by customer users to access Office 365 MT. Service accounts are used by various services to authenticate to servers and other services. |

### AC-4 Information Flow Enforcement (M) (H)

The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies].

| AC-04 | Control Summary Information |
| --- | --- |
| Responsible Role: Customer Administrator, Service Engineer Operations | |
| Parameter AC-04:  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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AC-04 - What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility:**  Government customers are responsible for ensuring that no information with a security impact level greater than moderate is stored, processed, or transmitted via the services provided to them by Office 365 MT; Office 365 MT will be accredited to store, process, and transmit up to Moderate Impact information as defined by NIST SP 800-60.  Non-government customers are responsible for ensuring that information stored, processed, or transmitted via the services provided to them by Office 365 MT is appropriate and in compliance with the risk policies of their organization.  Customer Lockbox is an optional feature that customers can use for controlling the flow of information in EXO. This feature allows customers to control Microsoft administrators' ability to access their content. If in response to a customer support request, a Microsoft administrator needs access to customer content, that Microsoft administrator initiates a Just In Time request which is routed to a customer administrator; this is in addition to the normal internal required access approvals. The customer administrator can then approve or deny this request via the customer administrator portal. Note that even if customers choose not to use this tool, Office 365 Information Security Policy is to never access customer content unless initiated by a customer request, and access to this data is always restricted to screened personnel with required JIT approvals. Customer Lockbox places the technical enforcement of this policy within the customer's direct control.  For additional information, see: https://support.office.com/en-us/article/Office-365-customer-lockbox-requests-36f9cdd1-e64c-421b-a7e4-4a54d16440a2  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT has current Interconnection Security Agreements (ISAs) for all external information systems connected to the application: Akamai, Commerce Platform Group (Universal Store), Cosmos, Office 365 Support, Azure, and Core Services Engineering (CSE) Corpnet.  Office 365 MT implements information flow control by allowing only connections and communication which are necessary to allow systems to operate, blocking all other ports, protocols and connections by default. This includes intra-service communications as well as connections to external information systems. Access Control Lists (ACLs) are the preferred mechanism to restrict network communications by source and destination networks, protocols, and port numbers.  Office 365 MT manages ACL and other firewall rule changes through the same configuration management processes as code changes, which includes review and approval steps. ACLs are stored in Office 365's source code repository, Source Depot. ACL changes are implemented to the networking devices through various tools and APIs, including NetConf and Azure management API's.  The use of firewall rules and ACLs allows Office 365 MT to control the flow of information within the system and between interconnected systems.  A detailed diagram of the Office 365 MT dataflow, which includes all internal and external information flows, is included in Section 10 of this SSP. |

#### AC-4 (21) Control Enhancement (M) (H)

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

| AC-04(21) | Control Summary Information |
| --- | --- |
| Responsible Role: Service Engineer Operations | |
| Parameter AC-04(21):  1. TLS and Active Directory Organizational Units; 2. 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AC-04(21) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT 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. Additionally, each Office 365 MT customer is placed in a separate Organizational Unit (OU) within Active Directory. Customer content within Office 365 MT is always tied to the customer’s specific OU, and Office 365 MT will only grant access to the data if there is a valid ticket from AAD authorizing access to the OU and the specific data. For a detailed discussion of how Office 365 MT separates flows and tenant data, please see Microsoft Office 365 Tenant Separation. |

### AC-5 Separation of Duties (M) (H)

The organization:

1. Separates [Assignment: organization-defined duties of individuals];
2. Documents separation of duties of individuals; and
3. Defines information system access authorizations to support separation of duties.

AC-5 Additional FedRAMP Requirements and Guidance:

Guidance: CSPs have the option to provide a separation of duties matrix as an attachment to the SSP. Directions for attaching the Separation of Duties Matrix document may be found in Section 15.11 ATTACHMENT 11 - Separation of Duties Matrix.

| AC-05 | Control Summary Information |
| --- | --- |
| Responsible Role: Customer Administrator, Program Manager | |
| Parameter AC-05(a):  code check-in and deployment duties; production access and audit configuration duties; access requesting and access granting capabilities | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AC-05 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility:**  All customers, including government and non-government customers, are responsible for separating duties of their organizational users as necessary, to prevent malevolent activity without collusion in compliance with their organizational policies.  Government and non-government customers using ADFS will manage their user accounts in their existing Active Directory infrastructure. For more information on managing user accounts in Active Directory, see TechNet article #754661: http://technet.microsoft.com/en-us/library/cc754661.aspx  Non-government customers not using ADFS will manage their user accounts in AAD via SUE. For more information on managing customer accounts via the SUE portal, see the following link: http://technet.microsoft.com/en-us/library/office-365-user-account-management.aspx  **DNS, OLM, OSI, SFB, SWE:**  All Office 365 MT service teams have defined roles as part of a comprehensive role-based access control mechanism described in control AC-2. Additionally, each service team has identified any roles that, if shared by a single person, would allow for malicious activity without collusion. When such role pairs exist, no individual is allowed to belong to both roles. Account permissions and role access are reviewed as part of the quarterly account review process.  **Bing, Delve, EXO, IP, MSTeams, SPO, SUE, WAC:**  Service team administrators are assigned to roles, which have a defined list of available permissions (RBAC). The separation of duties is documented through eligibilities (roles) assigned to service team administrators in account management tools.  By default, no accounts have active permissions to the production environment. If a service team administrator needs access to the production environment to perform a specific action, they must request that access and provide a business justification using JIT tools. A different service team administrator with the access approver role then reviews and either approves or denies the type of access requested. Access is only provided for a finite period of time based on the expected duration of the work to be performed. If access is approved, the JIT tools assign the service team administrator the minimum permissions required to perform the work and automatically revoke permissions at the end of the specified time period.  Implementing access control using JIT tools effectively prevents malevolent activity without collusion, as an individual has to review and approve the requestor's access request and would deny requests that would violate separation of duties requirements. |
| Part b | **Customer Responsibility:**  All customers, including government and non-government customers, are responsible for documenting separation of duties, in compliance with their organizational policies.  **DNS, OLM, OSI, SFB, SWE:**  The separation of duties is documented through eligibilities (roles) assigned to service team administrators in account management tools.  **Bing, Delve, EXO, IP, MSTeams, SPO, SUE, WAC:**  The separation of duties is documented through eligibilities (roles) assigned to service team administrators in account management tools, and additionally using JIT Tool elevations when privileged access is necessary. |
| Part c | **Customer Responsibility:**  All customers, including government and non-government customers, are responsible for separating duties of their organizational users as necessary, to prevent malevolent activity without collusion in compliance with their organizational policies.  Government and non-government customers using ADFS will manage their user accounts in their existing Active Directory infrastructure. For more information on managing user accounts in Active Directory, see TechNet article #754661: http://technet.microsoft.com/en-us/library/cc754661.aspx  Non-government customers not using ADFS will manage their user accounts in AAD via SUE. For more information on managing customer accounts via the SUE portal, see the following link: http://technet.microsoft.com/en-us/library/office-365-user-account-management.aspx  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Access authorization to support separation of duties is implemented through authorized role membership. Role membership is managed using account management tools. |

### AC-6 Least Privilege (M) (H)

The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

| AC-06 | Control Summary Information |
| --- | --- |
| Responsible Role: Customer Administrator, Program Manager, 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AC-06 - What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility:**  All customers, including government and non-government customers, are responsible for employing the concept of least privilege, allowing only authorized accesses for government and non-government customer users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions in compliance with their organizational policies.  Government and non-government customers using ADFS will manage their user accounts in their existing Active Directory infrastructure. For more information on managing user account permissions in Active Directory, see TechNet article #754661: http://technet.microsoft.com/en-us/library/cc754661.aspx  Non-government customers not using ADFS will manage their user accounts in AAD via SUE. For more information on managing account permissions via the SUE portal, see the following link: http://technet.microsoft.com/en-us/library/office-365-user-account-management.aspx  **DNS, OLM, OSI, SFB, SWE:**  Office 365 MT service teams employ the concept of least privilege, allowing only authorized accesses for service team users (and processes acting on behalf of service team users) that are necessary to accomplish assigned tasks in accordance with business functions and organizational need.  Service owners must employ the concept of least privilege for specific duties and information systems in accordance with risk assessments and as necessary to adequately mitigate risk to operational assets, individuals, and/or other organizations.  Each service team is responsible for defining least privileged roles within their team. Roles are documented within Microsoft account management tools.  **Bing, Delve, EXO, IP, MSTeams, SPO, SUE, WAC:**  By default, service team accounts belong to a security group that only has remote metadata access to the environment for that service team. This does not permit direct environment access, or access to customer content. If a service team administrator needs other privileges to the production environment, they must request that access and provide a business justification using JIT tools. A service team administrator with the access approver role then reviews and approves or denies the type of access requested. Access is only provided for a finite period of time based on the expected duration of the work to be performed. If access is approved, the JIT tool assigns the service team administrator to security groups with the minimum permissions required to perform the work and automatically revokes permissions at the end of the specified time period.  Reviews of accounts and all approved access occur quarterly. The use of this Just-In-Time permissions model ensures that service team administrators only ever have the least privileges required to accomplish assigned tasks in support of Office 365 MT mission and business functions, restricted by elevation level, resource access, and time. |

#### AC-6 (1) Control Enhancement (M)

The organization explicitly authorizes access to [Assignment: organization-defined security functions (deployed in hardware, software, and firmware) and security-relevant information].

| AC-06(1) | Control Summary Information |
| --- | --- |
| Responsible Role: Program Manager, Service Engineer Operations | |
| Parameter AC-06(1):  all 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AC-06(1) - What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility:**  Government customers are responsible for explicitly authorizing access to security functions, as defined by their organization, in compliance with their organizational policies, using their Active Directory (AD) infrastructure. Government users authenticate to government owned ADFS servers which utilize the government AD infrastructure to identify, authenticate, and apply permissions to that user’s session. The government ADFS server then communicates that identification/authentication and the associated permissions to AAD via SAML2.0 ticket.  For more information on managing user accounts in Active Directory, see TechNet article #754661: http://technet.microsoft.com/en-us/library/cc754661.aspx  Non-government customers can explicitly authorize access to security functions following the same procedures outlined for government customers, or they can elect to manage user accounts in AAD via SUE. For customers using AAD, the customer is responsible for authorizing access to "tenant administration" privileges which are used to manage user accounts and system configuration via the SUE portal.  For more information on managing account privileges via the SUE portal, see the following link: http://technet.microsoft.com/en-us/library/office-365-user-account-management.aspx  **DNS, OLM, OSI, SFB, SWE:**  Service teams employ the concept of least privilege, allowing only pre-authorized accesses for service team users (and processes acting on behalf of service team users) which are necessary to accomplish assigned tasks in accordance with business functions and organizational need.  Service owners employ the concept of least privilege for specific duties and information systems (including specific ports, protocols, and services) in accordance with risk assessments and as necessary to adequately mitigate risk to operational assets, individuals, and/or other organizations.  All access to the Office 365 MT system must be explicitly authorized, including the following security related functions: establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and system and security administration. Role owners are responsible for reviewing and approving role assignments, and roles are tailored for different job functions such that personnel only have the minimum access required to perform their duties.  **Bing, Delve, EXO, IP, MSTeams, SPO, SUE, WAC:**  By default, service team accounts belong to a security group that only has user-level operating system access to the production environment for that service team--this does not permit access to customer content. Access to any higher level of permissions must be requested through JIT tools and authorized by the on-call approver. This includes access to the following security functions: setting events to be audited, and system and security administration.  Role owners are responsible for reviewing and approving role assignments, and roles are tailored for different job functions such that personnel only have the minimum access required to perform their duties. Through the use of this Just-In-Time model, Office 365 MT explicitly authorizes access to security functions. |

#### AC-6 (2) Control Enhancement (M) (H)

The organization requires that users of information system accounts, or roles, with access to [FedRAMP Assignment: all security functions], use non-privileged accounts or roles, when accessing non-security functions.

AC-6 (2) Additional FedRAMP Requirements and 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-06(2) | Control Summary Information |
| --- | --- |
| Responsible Role: Program Manager | |
| Parameter AC-06(2):  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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AC-06(2) - What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility:**  Government customers are responsible for requiring that users of information system accounts/roles with access to government security functions or security-relevant information use non-privileged accounts/roles when accessing other system functions. Government customers are also responsible for auditing any use of privileged accounts/roles for such functions, in compliance with their organizational policies, using their Active Directory (AD) infrastructure. Government users authenticate to government managed ADFS servers which utilize the government AD infrastructure to identify, authenticate, and apply permissions to that user’s session. The government ADFS server then communicates that identification/authentication and the associated permissions to AAD via SAML2.0 ticket.  For more information on managing user accounts in Active Directory see TechNet article #754661: http://technet.microsoft.com/en-us/library/cc754661.aspx  Non-government customers can require that non-government customer users of information system accounts/roles with access to security functions or security-relevant information use non-privileged accounts/roles when accessing other system functions. Non-government customers can also audit any use of privileged non-government customer accounts/roles for such functions following the same procedures outlined for government customers, or they can elect to manage non-government customer user accounts in AAD via SUE. For customers using AAD, the customer is responsible for authorizing access to "tenant administration" privileges which are used to manage user accounts and system configuration via the SUE portal. Customers can elect to create a separate, non-privileged account for their administrative personnel to access other functions of Office 365 MT. AAD audits all actions taken by tenant administration accounts; audit logs are retained for 90 days.  For more information on managing customer account privileges via the SUE portal, see the following link: http://technet.microsoft.com/en-us/library/office-365-user-account-management.aspx  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Service teams require all individuals with administrative privileges to use their assigned accounts for performing business and security administrative functions in the production environment. Office 365 MT requires that service team administrators of information system accounts or roles with access to security functions or security-relevant information use non-MT accounts or roles when accessing other system functions. |

#### AC 6 (5) Control Enhancement (M) (H)

The organization restricts privileged accounts on the information system to [Assignment: organization-defined personnel or roles].

| AC-06(5) | Control Summary Information |
| --- | --- |
| Responsible Role: Customer Administrator, Office 365 Security Manager, Office 365 Trust Program Manager, Service Engineer Operations | |
| Parameter AC-06(5):  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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AC-06(5) - What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility:**  Government and non-government customers are responsible for restricting access to personnel and roles identified by the customer.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT restricts privileged access to the system to the internal roles identified and approved in account management tools. |

#### AC-6 (9) Control Enhancement (M) (H)

The information system audits the execution of privileged functions.

| AC-06 (9) | Control Summary Information |
| --- | --- |
| Responsible Role: Service Engineer Operations, Office 365 Security Manager, Office 365 Trust Program Manager, Customer Administrator | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AC-06 (9) - What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility:**  Government and non-government customers using ADFS are responsible for auditing account creation, modification, disabling, and deletion events for their Active Directory infrastructure as these events also pertain to Office 365 MT access. For these events, these customers are responsible for capturing what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event. Customers using Windows servers to support their ADFS infrastructure automatically meet this requirement as Windows captures these event details by default. For more information regarding Windows event logging, see the following link:  http://technet.microsoft.com/en-us/library/cc765981.aspx  Non-government customers not using ADFS do not have responsibility to produce audit records for Office 365 MT.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT includes the execution of privileged functions in the list of events to be audited by the system.  All commands run by all accounts are logged. No non-privileged actions (for example, browsing the public internet, use of email clients, etc.) are allowed within the production environment. Additionally, some teams use just in time (JIT) tools to allow privileged access to be granted within the production environment. Execution of privileged functions using JIT tools is audited. |

#### AC-6 (10) Control Enhancement (M) (H)

The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

| AC-06(10) | Control Summary Information |
| --- | --- |
| Responsible Role: Customer Administrator, Office 365 Security Manager, Office 365 Trust Program Manager, 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AC-06(10) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT does not have non-privileged users on the system. Office 365 MT prevents non-privileged users from accessing privileged functions. Customers do not have access to any functionality related to Office 365 MT safeguards/countermeasures. |

### AC-7 Unsuccessful Login Attempts (L) (M)

The organization:

1. Enforces a limit of [FedRAMP Assignment: not more than three (3)] consecutive invalid logon attempts by a user during a [FedRAMP Assignment: fifteen (15) minutes]; and
2. Automatically [Selection: locks the account/node for a [FedRAMP Assignment: thirty (30) minutes]; delays next logon prompt according to [Assignment: organization-defined delay algorithm]] when the maximum number of unsuccessful attempts is exceeded.

| AC-07 | Control Summary Information |
| --- | --- |
| Responsible Role: Customer Administrator, Office 365 Security Manager, Office 365 Trust Program Manager | |
| Parameter AC-07(a):  1. 10; 2. 15-minute period | |
| Parameter AC-07(b):  1. locks the account for 30 minutes; 2. according to AD Group Policy | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AC-07 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility:**  Government and non-government customers using ADFS are responsible for enforcing a limited number of consecutive invalid login attempts by a user during a defined time period in compliance with their organizational policies (not more than three attempts in 15 minutes for FedRAMP compliance). These customers will manage their account lockout policies in their existing Active Directory infrastructure. For information regarding account lockout policies, see the following link: http://technet.microsoft.com/en-us/library/hh994563%28v=ws.10%29.aspx  For non-government customers not using ADFS, account lockout policy is defined by AAD. For more information, see the following TechNet article: http://technet.microsoft.com/library/jj943764.aspx  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT has implemented an integrated defense against brute force attacks on privileged accounts rather than enforcing the FedRAMP recommendation of locking an account after 3 failed attempts in 15 minutes using AD Group Policy. This alternative implementation leverages the PIN lockout features on the hardware multifactor authentication token (smartcard), to enforce a lockout on 10 consecutive failed attempts regardless of time. Once triggered, the smartcard is locked until the engineer executes a successful PIN reset, which requires an alternate multifactor authentication and results in an email notification to the engineer’s manager. All Office 365 MT remote administration requires multifactor authentication.  Office 365 MT has adopted this alternative implementation as an operational requirement in order to ensure that customers have the ability to implement an organizationally specified policy for these same account settings. In addition, engineer accounts in the Office 365 domains (including the just in time (JIT) account created when an engineer needs elevated privileges) have machine generated random 15-character passwords which significantly decreases the potential threat of a brute force attempt.  A complete discussion of these risks and the mitigating controls in place are documented in the “Account Lockout Threshold and Period (AC-7(a))” Decision Log. |
| Part b | **Customer Responsibility:**  Government and non-government customers using ADFS are responsible for locking a user account that has had too many consecutive failed logins, in compliance with their organizational policies, using their Active Directory (AD) infrastructure (for at least thirty minutes to comply with FedRAMP requirements). These customers will manage their account lockout policies in their existing Active Directory infrastructure. For information regarding account lockout policies, see the following link: http://technet.microsoft.com/en-us/library/hh994563%28v=ws.10%29.aspx  For non-government customers not using ADFS, account lockout policy is defined by AAD. For more information, see the following TechNet article: http://technet.microsoft.com/library/jj943764.aspx  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT automatically locks accounts for at least 30 minutes when the maximum number of unsuccessful login attempts is exceeded. This value is set via AD Group Policy and is enforced by AD. |

### AC-8 System Use Notification (L) (M) (H)

The information system:

1. Displays to users [Assignment: organization-defined system use notification message or banner (FedRAMP Assignment: see additional Requirements and Guidance)] before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that:
   1. Users are accessing a U.S. Government information system;
   2. Information system usage may be monitored, recorded, and subject to audit;
   3. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and
   4. Use of the information system indicates consent to monitoring and recording;
2. Retains 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 information system; and

For publicly accessible systems:

Displays system use information [Assignment: organization-defined conditions (FedRAMP Assignment: see additional Requirements and Guidance)], before granting further access;

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

Includes a description of the authorized uses of the system.

AC-8 Additional FedRAMP Requirements and Guidance:

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.

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.

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.

| AC-08 | Control Summary Information |
| --- | --- |
| Responsible Role: Customer Administrator, Office 365 Security Manager, Office 365 Trust Program Manager, Service Engineer Operations | |
| Parameter AC-08(a)(1):  Organization-defined notification message or warning banner that contains the following elements:  1. Users are accessing a U.S. Government information system;  2. Information system usage may be monitored, recorded, and subject to audit;  3. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and  4. Use of the information system indicates consent to monitoring and recording | |
| Parameter AC-08(a)(2):  Organization-defined notification message or warning banner that contains the following elements:  1. Users are accessing a U.S. Government information system;  2. Information system usage may be monitored, recorded, and subject to audit;  3. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and  4. Use of the information system indicates consent to monitoring and recording | |
| Parameter AC-08(a)(3):  Organization-defined notification message or warning banner that contains the following elements:  1. Users are accessing a U.S. Government information system;  2. Information system usage may be monitored, recorded, and subject to audit;  3. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and  4. Use of the information system indicates consent to monitoring and recording | |
| Parameter AC-08(a)(4):  Organization-defined notification message or warning banner that contains the following elements:  1. Users are accessing a U.S. Government information system;  2. Information system usage may be monitored, recorded, and subject to audit;  3. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and  4. Use of the information system indicates consent to monitoring and recording | |
| Parameter AC-08(c)(1):  included in the terms of service | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AC-08 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility:**  Government customers are responsible for displaying an approved system use notification message or banner on the authentication page served by their ADFS server used to authenticate to Office 365 MT that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that: (i) users are accessing a U.S. Government information system; (ii) system usage may be monitored, recorded, and subject to audit; (iii) unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) use of the system indicates consent to monitoring and recording.  Non-government customers using ADFS can implement an approved system use notification message or banner before granting access to ADFS. Non-government customers not using ADFS may implement system use notification messages or banners on their local workstations.  **Part 1,2,3,4:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  All service teams include a FISMA warning banner prior to administrative login to all servers. There are two approved messages reviewed by Microsoft Corporate, External, and Legal Affairs (CELA). The first reads:  "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 Office 365 environment:  • Maintain their remote computer in a secure manner, in accordance with organizational security policies and procedures as defined in Microsoft Remote Connectivity Security Policies.  • Only access the Office 365 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 Office 365 environment data exceeding a FIPS 199 Moderate security categorization (FISMA Controlled Unclassified Information)."  A second, alternate approved message 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 Office 365 environment:  (1) shall maintain their remote computer in a secure manner, in accordance with organizational security policies and procedures as defined in Microsoft Remote Connectivity Security Policies;  (2) shall only access the Office 365 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 Office 365 environment data exceeding a FIPS 199 Moderate security categorization (FISMA Controlled Unclassified Information)." |
| Part b | **Customer Responsibility:**  Government customers are responsible for retaining the notification message or banner on the screen until users take explicit actions to log on to Office 365 MT using the customer's ADFS server.  Non-government customers can retain the notification message or banner on the screen until users take explicit actions to log on to workstations used to access Office 365 MT, consistent with organizational policies and risk tolerances.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The warning banner is displayed during the production environment logon sequence. Service team administrators must acknowledge the usage conditions and take explicit action to complete the login sequence. |
| Part c | **Customer Responsibility:**  Government customers are responsible for displaying an approved system use notification message or banner on the authentication page served by their ADFS server used to authenticate to Office 365 MT that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that: (i) users are accessing a U.S. Government information system; (ii) system usage may be monitored, recorded, and subject to audit; (iii) unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) use of the system indicates consent to monitoring and recording.  Non-government customers using ADFS can implement an approved system use notification message or banner before granting access to ADFS. Non-government customers not using ADFS may implement system use notification messages or banners on their local workstations.  **Part 1,2,3:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT does not display a warning banner on customer interfaces. Based on review of FedRAMP requirements, and discussions and confirmation with Office 365 MT environment process owners, this control is not applicable to the Office 365 MT environment. Customers are responsible for implementing this control on their ADFS authentication page.  Office 365 MT considers not implementing a banner to be an operational requirement for a commercial service. Office 365 MT does provide links to both privacy and legal information related to Office 365 MT on the public-facing Office 365 MT login page. |

Additional FedRAMP Requirements and Guidance

Requirement 1: 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 2: 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. 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.

Requirement 3: 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.

| AC-08 Req. | Control Summary Information |
| --- | --- |
| Responsible Role: Service Engineer Operations, Office 365 Trust Program Manager | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AC-08 Req. - What is the solution and how is it implemented? | |
| --- | --- |
| Req. 1 | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT does not display a warning banner on customer interfaces. Based on review of FedRAMP requirements, discussions and confirmation with Office 365 MT environment process owners, this control is not applicable to the Office 365 MT environment because Office 365 MT is a commercial service and customers will be responsible for implementing this control on their ADFS authentication page. Office 365 MT considers this to be an operational requirement for a commercial service. |
| Req. 2 | **Customer Responsibility:**  Government customers are responsible for verifying the notification message or banner on the ADFS login page used to authenticate government customer users to Office 365 MT at an interval consistent with organizational policies.  Non-government customers can verify the notification message or banner on the workstations used to access Office 365 MT, consistent with organizational policies and risk tolerances.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT does not display a warning banner on customer interfaces. |
| Req. 3 | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT does not display a warning banner on customer interfaces. |

### AC-10 Concurrent Session Control (M) (H)

The information system limits the number of concurrent sessions for each [Assignment: organization-defined account and/or account type] to [FedRAMP Assignment: three (3) sessions for privileged access and two (2) sessions for non-privileged access].

| AC-10 | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager, Service Engineer Operations | |
| Parameter AC-10:  1. Service team accounts; 2. one session | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AC-10 - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT servers restrict concurrent sessions to one session per service team administrator per server. The TSGs, or SSH Gateways for Linux servers, are configured to allow single concurrent sessions, or three concurrent sessions for SSH Gateways, for users to those devices. TSGs do not allow multiple sessions, but instead allow service team administrators to connect to multiple servers concurrently, using a single session per server, so that administrators can effectively perform their duties. Service team administrators do not have any permissions on the TSGs themselves. The TSG is only used to enforce multifactor authentication and encryption requirements. Once the service team administrator connects to a specific server through a TSG, the specific server will enforce a session limit of one per administrator. SSH Gateways enforce a concurrent session limit of three sessions. Service team administrators do not have any permissions on the SSH Gateway themselves. The SSH Gateway is only used to enforce multifactor authentication and encryption requirements. |

### AC-11 Session Lock (M) (H)

The information system:

1. Prevents further access to the system by initiating a session lock after [FedRAMP Assignment: fifteen (15) minutes] of inactivity or upon receiving a request from a user; and
2. Retains the session lock until the user reestablishes access using established identification and authentication procedures.

| AC-11 | Control Summary Information |
| --- | --- |
| Responsible Role: Customer Administrator, Office 365 Security Manager, Office 365 Trust Program Manager, Program Manager | |
| Parameter AC-11(a):  15-minute 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AC-11 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility:**  Government customers are responsible for preventing further access to the system by initiating a session lock, after a given period of user inactivity at the workstation level, in compliance with organizational policies.  Non-government customers can prevent further access to the system by initiating a session lock, after a given period of user inactivity at the workstation level, in compliance with organizational policies.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Server sessions are locked after no more than 15 minutes of inactivity by GPO, or upon user request. SSH Gateways used for Linux server sessions also enforce a session timeout after 15 minutes of inactivity. |
| Part b | **Customer Responsibility:**  Government customers are responsible for retaining the session lock until the user reestablishes access using established identification and authentication procedures, in compliance with organizational policies.  Non-government customers can retain the session lock until the user reestablishes access using established identification and authentication procedures, in compliance with organizational policies.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 MT user must re-authenticate into the system once the user session has been locked for inactivity. |

#### AC-11 (1) Control Enhancement (M) (H)

The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image.

| AC-11(1) | Control Summary Information |
| --- | --- |
| Responsible Role: Customer Administrator | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AC-11(1) - What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility:**  Government customers are responsible for enforcing that the session lock mechanism, when activated on a device with a display screen, places a publicly viewable pattern onto the associated display, hiding what was previously visible on the screen.  Non-government customers can enforce that the session lock mechanism, when activated on a device with a display screen, places a publicly viewable pattern onto the associated display, hiding what was previously visible on the screen.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI,SFB, SPO, SUE, SWE, WAC:**  All Terminal Services Gateways (TSG) run Windows. Compliance with this control is a built-in feature of Microsoft Windows. Microsoft Windows places a publicly-viewable pattern onto the associated display when the session lock mechanism is activated on a device with a display screen, hiding what was previously visible on the screen.  For teams using Linux, when connecting through an SSH gateway, Office 365 MT engineers use machines which have password enabled screensavers. Engineers are responsible for agreeing to a Secure Work Environment Attestation affirming that only securely configured workstations may be used. |

### AC-12 Session Termination (M) (H)

The information system automatically terminates a user session after [Assignment: organization-defined conditions or trigger events requiring session disconnect].

| AC-12 | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager, Office 365 Trust Program Manager, Program Manager | |
| Parameter AC-12:  logout request initiated by user for customer users, and after logout request initiated by user or 24 hours of inactivity for service team 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AC-12 - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT automatically terminates customer and service team administrator sessions upon receiving a logout request, or after 24 hours. Additionally, service team administrator sessions are disconnected after no more than 15 minutes of inactivity. |

### AC-14 Permitted Actions without Identification or Authentication (L) (M) (H)

The organization:

1. Identifies [Assignment: organization-defined user actions] that can be performed on the information system without identification or authentication consistent with organizational missions/business functions; and
2. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification or authentication.

| AC-14 | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager, Office 365 Trust Program Manager, Service Engineer Operations | |
| Parameter AC-14(a):  all user 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AC-14 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility:**  All customers, including government and non-government customers, are responsible for identifying specific user actions that can be performed on the information system without identification or authentication in compliance with organizational policies.  Guest access to SFB meetings, if enabled, allows anyone with a meeting invite to access the meeting lobby. The meeting organizer is responsible for establishing the identity of lobby participants before granting them access to the meeting.  Government customers are responsible for disabling guest access to SFB meetings to remain compliant with FedRAMP standards as advised in "Office 365 MT Government Compliance Considerations v 2 00".  Non-government customers are responsible for determining if the use of guest access to SFB meetings should be allowed for their organization. This setting can be configured by government and non-government customers. For more information, see the following TechNet article: http://technet.microsoft.com/en-US/library/gg398648.aspx  **DNS:**  Office 365 DNS will respond to unauthenticated DNS queries. This is required to be compliant with the DNS specification and to ensure customers can successfully resolve Office 365 URLs.  **Bing, Delve, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT does not allow any actions to be performed on the system without identification and authentication.  The only actions permitted by Office 365 MT to be performed on the system without authentication are accessing the Legal, Privacy, and Feedback option on the customer facing welcome page. |
| Part b | **Customer Responsibility:**  All customers, including government and non-government customers, are responsible for documenting and providing supporting rationale for user actions not requiring identification and authentication in compliance with organizational policies.  Guest access to SFB meetings, if enabled, allows anybody with a meeting invite to access the meeting lobby. The meeting organizer is responsible for establishing the identity of lobby participants before granting them access to the meeting.  Government customers are responsible for disabling guest access to SFB meetings to remain compliant with FedRAMP standards as advised in "Office 365 MT Government Compliance Considerations".  Non-government customers are responsible for determining if the use of guest access to SFB meetings should be allowed for their organization. This setting can be configured by government and non-government customers. For more information, see the following TechNet article: http://technet.microsoft.com/en-US/library/gg398648.aspx  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The information in the Legal, Privacy, and Feedback options on the customer facing welcome page is either legally required or foundational to an internet facing cloud service and none of it impacts the security of the system if publicly disclosed. |

### AC-17 Remote Access (L) (M) (H)

The organization:

1. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and
2. Authorizes remote access to the information system prior to allowing such connections.

| AC-17 | Control Summary Information |
| --- | --- |
| Responsible Role: Customer Administrator, Office 365 Security Manager, Office 365 Trust Program Manager, Program Manager, 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AC-17 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility:**  Customers connect to Office 365 MT via the following allowed methods of remote access: web interface via web browser, email client, SFB software client, or PowerShell client. These methods are documented in “Office 365 MT Government Compliance Considerations”.  Government customers are responsible for ensuring that client software is configured to only establish sessions using FIPS 140-2 compliant protocols. This can be accomplished by restricting access to the government customer’s ADFS to only internal network traffic. This will force government customers attempting to connect to Office 365 MT to VPN into the customer’s network or directly be on the network at the time of authentication. When the customer connects (directly or via VPN) to the network it should perform a health inspection that validates USGCB baselines including browser settings to require FIPS 140-2 connections.  For more information about configuring customer ADFS server(s) to only allow connections from customer internal networks, see the following TechNet article: http://technet.microsoft.com/en-us/library/hh526961(v=ws.10).aspx  Non-government customers should adhere to their respective regulatory and internal policies but may not be required to use FIPS 140-2 compliant encryption, and Office 365 MT will accept non-FIPS 140-2 compliant requests. Because of the need to support customers with out-of-date software, Office 365 MT does not enforce FIPS 140-2 compliant encryption for all customers.  **Bing, Delve, EXO, IP, MSTeams, OSI, SFB, SPO, SUE, SWE, WAC:**  Each service team implements remote access through the use of a Terminal Services Gateway (TSG) to gain remote access to Office 365 MT. Methods of remote access are documented in the decision log "Authorizing Remote Access For O365 Staff (AC-17)". Government customers do not have access to authenticate to MT via the TSGs.  Usage restrictions and connection/configuration requirements for Office 365 MT personnel are established in the Terminal Services Gateways by Active Directory-managed Group Policy. These policies include the bulleted implementation guidance of configuration/connection requirements listed below and are available for review:  • TSG servers are configured to only use FIPS 140-2 compliant encryption  • TSG sessions are configured to disconnect after 15 minutes of inactivity  • TSG sessions are configured to automatically log off after 24 hours, terminating the network session  **DNS:**  DNS uses TSGs in the Global Management Environment (GME), which is managed by Azure and is part of Azure’ accreditation boundary.  **OLM:**  Remote access to the Linux servers is through an SSH gateway tied to Torus and JIT. An engineer elevates against Torus using a Yubikey with PIN+touch policy. Elevation request parameters are signed with the Yubikey’s private key to guarantee that request came from the engineer who owns the Yubikey. After approval is granted, Torus sends the required authentication certificates to the engineer, and the certificate is tied to the YubiKey. Using the YubiKey with PIN+touch policy and certificates, the engineer then accesses the gateway. Remote access to the PAVC scanner is done using CJIS and RDP. |
| Part b | **Customer Responsibility:**  Remote access is how customers are expected to interact with Office 365 MT. Office 365 MT expects all government and non-government customers to have remote access. Customers are responsible for authorizing their users to access Office 365 MT and in doing so authorize them to use the system remotely. By default, customers do not have remote access to Office 365 MT until an account is created for them by their customer administrator.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  All approved maintenance activities are authorized for execution via remote access to the Office 365 MT environment. The system devices reside in data centers geographically segregated from the operations teams. Personnel local to the data centers do not have logical access to information system components. As a result, the only way to perform maintenance is remotely. Remote access is controlled by RBAC and requires approval before placement into security groups tied to remote access. |

#### AC-17 (1) Control Enhancement (M) (H)

The information system monitors and controls remote access methods.

| AC-17(1) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager, Office 365 Trust Program Manager | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AC-17(1) - What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility:**  Government customers are responsible for employing automated mechanisms to facilitate the monitoring and control of remote access methods, in compliance with their organizational policies, using their Active Directory (AD) infrastructure. Government users authenticate to government owned ADFS servers which utilize the government AD infrastructure to identify, authenticate, and apply permissions to that user’s session. The government ADFS server then communicates that identification/authentication and the associated permissions to AAD via SAML2.0 ticket.  Non-government customers can employ automated mechanisms to facilitate the monitoring and control of remote access methods following the same procedures outlined for government customers, or they can elect to manage user accounts in AAD via SUE. For customers using AAD, AAD is the automated mechanism used to monitor and control remote access, using the settings defined by the client in the SUE portal. AAD retains audit logs of remote connections for 90 days.  For more information on managing customer accounts via the SUE portal, see the following link:  http://technet.microsoft.com/en-us/library/office-365-user-account-management.aspx  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  All remote access connections from service team personnel are audited utilizing the access points auditing functionality. The service team monitors the connections for attempted unauthorized use of Office 365 MT using Near Real Time Security Alerting tools.  Smartcard two-factor authentication through Terminal Service Gateways (TSGs) is the only approved method to gain remote administrative access to systems in any Office 365 MT domains.  Logs from remote access points and customer-facing interfaces are uploaded to a repository service, and reports are generated from those logs, in conjunction with the NRT Security Monitoring of remote access methods. |

#### AC-17 (2) Control Enhancement (M) (H)

The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

| AC-17(2) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager, Office 365 Trust Program Manager | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AC-17(2) - What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility:**  Government customers are responsible for configuring their workstations to support the use of cryptography to protect the confidentiality and integrity of remote access sessions in compliance with organizational policies. Government customers are also required to configure workstations to establish FIPS 140-2 validated TLS sessions for remote access in order to retain compliance with FedRAMP requirements. This can be accomplished by restricting access to the government customer’s ADFS to only internal network traffic. This will force government customers attempting to connect to Office 365 MT to VPN into the customer’s network or directly be on the network at the time of authentication.  When the customer connects (directly or via VPN) to the network it should perform a health inspection that validates USGCB baselines, including browser settings, requiring FIPS 140-2 connections. For more information about configuring customer ADFS server(s) to only allow connections from customer internal networks, see the following TechNet article: http://technet.microsoft.com/en-us/library/hh526961(v=ws.10).aspx  Non-government customers may configure their workstations to support the use of cryptography to protect the confidentiality and integrity of remote access sessions in compliance with organizational policies.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT uses FIPS 140-2 compliant cryptography to encrypt TSG connections to protect the confidentiality and integrity of remote access sessions.  FIPS encryption as handled by Microsoft products is further explained in TechNet article cc750357: https://technet.microsoft.com/en-us/library/security/cc750357.aspx  Office 365 MT’s FIPS 140-2 encryption modules used for transmitted information are certified by NIST via certificates 1892, 1893, 1894, 1895, 1896, 1897, 1898, 1899.  The non-inclusion of Windows Server 2012 on the updated list of validated FIPS 140-2 modules is solely due to the significant backlog of work required to update the Security Policy documents and submit Change Letters to NIST CMVP for Microsoft’s many FIPS 140-2 validation certificates. Windows Server 2012 provides and uses the AES\_CTR\_DRBG algorithm as the default deterministic random bit generator. Note the statement from http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-historical.htm:  “This does not mean that the overall FIPS-140 certificate has been revoked, rather it indicates that the certificate and the documentation posted with it do not accurately reflect how the module can be used in FIPS mode. Agencies may make a risk determination on whether to continue using the modules on this list based on their own assessment of where and when the RNG is used by the module.”  Again, the deprecated RNG is not in use by default in Windows Server 2008. Office 365 MT Support developers are prevented from choosing unapproved DRBG or RNG algorithms by the code reviewing processes described in the SA family of the SSP. |

#### AC-17 (3) Control Enhancement (M) (H)

The information system routes all remote accesses through [Assignment: organization-defined number] managed network access control points.

| AC-17(3) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager, Office 365 Trust Program Manager | |
| Parameter AC-17(3):  two pools of TSGs per data center | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AC-17(3) - What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility:**  Government customers are responsible for routing remote access traffic to Office 365 MT through a limited number of managed access points. Further information is available in CA-3(3).  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT Service teams implement remote access through the use of specially-configured Terminal Services Gateways (TSGs) or SSH Gateways for Linux servers, as the only approved way to gain remote administrative access to Office 365 MT service team systems. Each service team has a load-balanced pool of TSGs in two geographically-distributed data centers. As discussed in AC-17, SWE manages these TSGs for EXO, IP, SFB, SPO, SUE, SWE, and WAC. Azure manages TSGs for DNS. OSI disables remote access by default. OLM utilizes SSH Gateways.  In addition to access through the TSGs, teams may access certain administrative functionality on the production servers through the use of Remote PowerShell sessions. In order to do this, a user will be authorized for read only access to the production environment. Privilege escalation is enabled using a Just-In-Time (JIT) tool; this is the same way it is enabled for RDP, which uses JIT tools. There exists a load-balanced virtual IP at each data center which serves as a single point of access to the functionality enabled by this service. The cmdlets that can be executed are enumerated based on the privilege level identified in the access claim obtained during authentication. These cmdlets are the only administrative functionality that can be accessed and executed by users connecting using this method.  DNS uses Pulse VPN in the Global Management Environment (GME), which is managed by Azure and is part of Azure’ accreditation boundary. |

#### AC-17 (4) Control Enhancement (M) (H)

The organization:

1. Authorizes the execution of privileged commands and access to security-relevant information via remote access only for [Assignment: organization-defined needs]; and
2. Documents the rationale for such access in the security plan for the information system.

| AC-17(4) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager, Office 365 Trust Program Manager | |
| Parameter AC-17(4)(a):  support of the operational 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AC-17(4) - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT authorizes remote access for Office 365 MT service team users. Because Office 365 MT service teams do not have physical access to data centers, there is a business requirement for those personnel to have remote access. This business decision is documented in "Authorizing Remote Access For O365 Staff (AC-17)".  Before service team personnel can connect to Office 365 MT remotely, they must first be approved for remote access by an authorized manager. This process is automatically enforced by Microsoft account management tools. |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The only way to manage the system is via the remote access regime described above in AC-17. Remote access to privileged functions has been approved by the system owner. Remote access is only allowed to support authorized maintenance and support activities. |

#### AC-17 (9) Control Enhancement (M) (H)

The organization provides the capability to expeditiously disconnect or disable remote access to the information system within [FedRAMP Assignment: fifteen (15) minutes].

| AC-17(9) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager, Office 365 Trust Program Manager | |
| Parameter AC-17(9):  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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AC-17(9) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT service team administrators do not have physical / local access to Office 365 MT production. As a result, all administrative access to Office 365 is remote. If remote access were disabled, Office 365 MT service team administrators would have no way to monitor or administer the service. Additionally, all customer access to Office 365 MT is remote due to the nature of cloud services.  The system has the capability of terminating a user session on the TSGs. First, the IDM account associated with the user must be disabled, then the session is terminated on the TSG. This prevents the user from further remote access of the system.  OSI disables remote access by default.  Management of the TSGs in use by DNS is inherited from Azure. |

### AC-18 Wireless Access Restrictions (L) (M) (H)

The organization:

1. Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; and
2. Authorizes wireless access to the information system prior to allowing such connections.

| AC-18 | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager, Office 365 Trust Program Manager | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AC-18 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility:**  Office 365 MT does not distinguish between wireless and non-wireless customer access. If government or non-government customers using ADFS wish to prevent wireless customer access, they can do so by configuring ADFS to only allow connections from domain-joined machines on a non-wireless network.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Azure establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access via the Network Security Standard, which explicitly prohibits the use of wireless in the Azure environment. |
| Part b | **Customer Responsibility:**  Office 365 MT does not distinguish between wireless and non-wireless customer access. If government or non-government customers using ADFS wish to prevent wireless customer access, they can do so by configuring ADFS to only allow connections from domain-joined machines on a non-wireless network.  **Bing, Delve DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Azure does not allow wireless access within Azure data centers. |

#### AC-18 (1) Control Enhancement (M) (H)

The information system protects wireless access to the system using authentication of [Selection (one or more): users; devices] and encryption.

| AC-18(1) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager, Office 365 Trust Program Manager | |
| Parameter AC-18(1):  users and 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AC-18(1) - What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility:**  Office 365 MT does not distinguish between wireless and non-wireless customer access. If government or non-government customers using ADFS wish to allow wireless customer access and authenticate devices and users, they are responsible for configuring their ADFS infrastructure to perform this authentication.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Azure does not allow wireless access within Azure data centers. |

### AC-19 Access Control for Portable and Mobile Systems (L) (M) (H)

The organization:

1. Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and
2. Authorizes the connection of mobile devices to organizational information systems.

| AC-19 | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager, Office 365 Trust Program Manager | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AC-19 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility:**  All customers, including government and non-government customers, are responsible for establishing usage restrictions, configuration and connection requirements, and implementation guidance for organization-controlled mobile devices used to connect to Office 365 MT.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  There are no mobile devices within the Office 365 MT boundary. Azure is responsible for preventing the physical connection of mobile devices to Office 365 MT servers.  The prevention of mobile devices connecting to Office 365 MT is inherited from Azure, which has a FedRAMP P-ATO (F1209051525) |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The prevention of mobile devices connecting to Office 365 MT is inherited from Azure, which has a FedRAMP P-ATO (F1209051525) |

#### AC-19 (5) Control Enhancement (M) (H)

The organization employs [Selection: full-device encryption; container encryption] to protect the confidentiality and integrity of information on [Assignment: organization-defined mobile devices].

| AC-19(5) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager, Office 365 Trust Program Manager | |
| Parameter AC-19(5):  1. full-device encryption; 2. all mobile 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AC-19(5) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  There are no mobile devices within the Office 365 MT boundary. |

### AC-20 Use of External Information Systems (L) (M) (H)

The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:

1. Access the information system from external information systems; and
2. Process, store, or transmit organization-controlled information using external information systems.

| AC-20 | Control Summary Information |
| --- | --- |
| Responsible Role: Customer Administrator, Azure, Office 365 Trust Program Manager | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AC-20 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility:**  All customers, including government and non-government customers, are responsible for establishing terms and conditions allowing authorized individuals to access Office 365 MT from customer controlled networks and workstations.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  All groups supporting Office 365 MT utilize Microsoft-issued external information systems (laptops, desktops, etc.). All personnel are required to maintain secure computer configurations.  Office 365 MT has Interconnection Security Agreements with Microsoft Core Services Engineering (CSE), Microsoft Azure, Microsoft Cosmos, Microsoft Universal Store and Microsoft Office 365 Support. Office 365 MT also has a Memorandum of Understanding (MOU) with Akamai. The security policy and ISAs/MOUs address the terms and conditions for accessing Office 365 MT data on these external platforms. Office 365 Trust is responsible for developing the ISAs/MOUs, which are reviewed annually.  With regard to trust relationships established with other organizations that own, operate, and/or maintain external information systems, vendors are required to use the Microsoft provided OS images which meet the requirements of Network Access Control/Network Access Protection (NAC/NAP) controls.  Through the use of these policies, vendor agreements, ISAs, and MOUs Office 365 MT establishes conditions for allowing access to Office 365 MT from external information systems. |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  See AC-20(a) |

#### AC-20 (1) Control Enhancement (M) (H)

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

1. Verifies the implementation of required security controls on the external system as specified in the organization’s information security policy and security plan; or
2. Retains approved information system connection or processing agreements with the organizational entity hosting the external information system.

| AC-20(1) | Control Summary Information |
| --- | --- |
| Responsible Role: Customer Administrator, Office 365 Trust Program Manager | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AC-20(1) - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility:**  All customers, including government and non-government customers, are responsible for verifying the implementation of organizationally required security controls on customer workstations in compliance with organizational policies.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Microsoft will not implement Network Access Protection (NAP) to enforce security requirements of hosts accessing the system via the internet. The functionality to support NAP has been deprecated. This is documented in the decision log “Access via external system AC-20(1)(a).” |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  All personnel accessing the environment via Microsoft-issued external information systems (laptops, desktops, etc.) agree to maintain their remote computer in a secure manner and in accordance with organizational security policies and procedures. Microsoft IT (MSIT) is responsible for enforcing compliance in accordance with the ISA between Office 365 MT and Microsoft IT. |

#### AC-20 (2) Control Enhancement (M) (H)

The organization [Selection: restricts; prohibits] the use of organization-controlled portable storage devices by authorized individuals on external information systems.

| AC-20(2) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager, Office 365 Trust Program Manager | |
| Parameter AC-20(2):  prohibits | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AC-20(2) - What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility:**  All customers, including government and non-government customers, are responsible for limiting the use of organization-controlled portable storage media by authorized individuals on customer workstations connected to Office 365 MT in compliance with organizational policies.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT prohibits any organization-controlled portable storage media. |

### AC-21 Information Sharing (M) (H)

The organization:

1. Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for [Assignment: organization-defined information sharing circumstances where user discretion is required]; and
2. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions.

| AC-21 | Control Summary Information |
| --- | --- |
| Responsible Role: Customer Administrator | |
| Parameter AC-21(a):  information sharing circumstances where user discretion is required | |
| Parameter AC-21(b):  automated mechanisms and manual processes | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AC-21 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility:**  Government and non-government customers may choose to share their information/content in accordance with their security policies and are responsible for enabling authorized customer users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information being shared.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT employees are not allowed to share Office 365 MT data or customer content outside the security boundary. |
| Part b | **Customer Responsibility:**  Government and non-government customers who choose to share their information/content are responsible for employing automated mechanisms or manual processes to assist users in making information sharing/collaboration decisions.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT employees are not allowed to share Office 365 MT data or customer content outside the security boundary and thus do not make discretionary sharing decisions. |

### AC-22 Publicly Accessible Content (L) (M) (H)

The organization:

1. Designates individuals authorized to post information onto a publicly accessible information system;
2. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information;
3. Reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included; and
4. Reviews the content on the publicly accessible information system for nonpublic information [FedRAMP Assignment: at least quarterly] and removes such information, if discovered.

| AC-22 | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Trust Program Manager | |
| Parameter AC-22(d):  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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AC-22 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **DNS:**  Office 365 DNS allows public requests to resolvers as this is a service requirement to ensure machines can properly resolve Office 365 URLs. Office 365 DNS also provides a web service for customers to programmatically maintain any customers' zones or vanity domains that have been implemented by customers. All connections to the web service are encrypted and partners are required to authenticate to the web service using Microsoft issued SSL certificates obtained through SSLAdmin.  **Bing, Delve, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT does not have any publicly accessible information systems. The only actions permitted by Office 365 MT to be performed on the system without authentication are accessing the Legal, Privacy Statement, Help, and Language Preference options on the welcome page. Office 365 MT has designated the Microsoft Content Management Team as the group authorized to make changes to this limited public information. |
| Part b | **DNS:**  Office 365 DNS provides a web service for customers to programmatically maintain any customers' zones or vanity domains that have been implemented by customers. All connections to the web service are encrypted and partners are required to authenticate to the web service using Microsoft issued SSL certificates obtained through SSLAdmin. In addition, the web service validates that update requests are not writing malformed data to DNS records prior to committing any changes.  **Bing, Delve, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The content of the information is vetted through the Microsoft Content Management Team which includes attorneys who are trained in screening public content for non-public content and are required to earn Continuing Professional Education credits (CPEs) to maintain their licenses. |
| Part c | **DNS:**  This does not apply to Office 365 DNS records as all aspects of DNS zones must be publicly accessible per the DNS specification.  **Bing, Delve, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  All information must go through the Microsoft Content Management Team for review prior to being posted to ensure nonpublic information is not made available. This review occurs as part of normal change management processes. |
| Part d | **DNS:**  This does not apply to Office 365 DNS records as all aspects of DNS zones must be publicly accessible per the DNS specification.  **Bing, Delve, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The PR/Marketing team conducts weekly scans on search engines and media web sites (Bing, Google, Twitter, Facebook) using keywords like Microsoft, Microsoft Data Center, competitor names, product names, etc. to identify any disclosed nonpublic information.  Additionally, all publicly available white papers are updated and reviewed by the Marketing and Communications team on a quarterly basis.  If any nonpublic information is identified as part of reviews, the Office 365 incident response process is followed to investigate and remediate the issue. |

* 1. Awareness and Training (AT)

### AT-1 Security Awareness and Training Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls; and
2. Reviews and updates the current:
   1. Security awareness and training policy [FedRAMP Assignment: at least every 3 years]; and
   2. Security awareness and training procedures [FedRAMP Assignment: at least annually].

| AT-01 | Control Summary Information |
| --- | --- |
| Responsible Role: Customer Administrator, Office 365 Trust Program Manager | |
| Parameter AT-01(a)(1):  Service Engineer Operations, Program Manager, Developer, Tester, Office 365 Trust Program Manager, Office 365 Security Manager, BCM | |
| Parameter AT-01(a)(2):  Service Engineer Operations, Program Manager, Developer, Tester, Office 365 Trust Program Manager, Office 365 Security Manager, BCM | |
| Parameter AT-01(b)(1):  annually | |
| Parameter AT-01(b)(2):  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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AT-01 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility:**  Government customers are responsible for developing and maintaining appropriate Awareness and Training policies that govern security awareness training activities for their organization and users.  **Part 1:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Information Security Policy defines Office 365 MT policies. This document addresses the purpose, scope, roles, responsibilities, compliance requirements, and required coordination among the various Microsoft organizations providing some level of support for the security of Office 365 MT. Policies are made available to personnel responsible for implementing awareness and training policies and procedures via SharePoint.  **Part 2:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Information Security Policy contains policies that must be met in the delivery and operation of Office 365 MT. Standards and Procedures to facilitate execution of these policies are documented in the Active Framework Controls, Office 365 Standard Operating Procedures (SOPs), and service team-specific SOPs. These standards and procedures act as adjuncts to the security policy and provide implementation level requirements and details to carry out specific operational tasks. A detailed mapping of Office 365 Standards and Procedures to each control is available. Office 365 SOPs are distributed to roles providing support for security awareness and training via SharePoint. |
| Part b | **Customer Responsibility:**  Government customers are responsible for annually updating Awareness and Training policies and procedures.  **Part 1:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Information Security Policy is reviewed and updated annually by the Office 365 Trust team.  **Part 2:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 SOPs are reviewed and updated annually. |

### AT-2 Security Awareness (L) (M) (H)

The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors):

1. As part of initial training for new users;
2. When required by information system changes; and
3. [FedRAMP Assignment: at least annually] thereafter.

| AT-2 | Control Summary Information |
| --- | --- |
| Responsible Role: Customer Administrator, Office 365 Trust Program Manager, Program Manager | |
| Parameter AT-02(c):  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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AT-2 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility:**  All customers, including government and non-government customers, are responsible for providing basic security awareness training to their employees and vendors as necessary, including training on basic security awareness training and role-based training, as appropriate per job description. This training shall include requirements that customer users not bypass Office 365 security through actions such as:  1. Improperly forwarding documentation through Exchange Online  2. Improperly securing documentation hosted in SharePoint Online  3. Circumventing, disabling, or downgrading session-level encryption.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 provides basic security and privacy awareness training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users. This is accomplished by requiring all staff to take a New Employee Orientation (NEO) security awareness training course, Standards of Business Conduct, within the first 30 days of their employment or transfer into the organization. This training course is facilitated by Microsoft Information Technology (MSIT) and Corporate Security, and encompasses standard business security measures, basic information security, and user actions to maintain security and to respond to suspected security incidents.  In addition, all staff are required to take security and privacy awareness training annually after their initial training. Office 365 has implemented the security training control by requiring all new users (employees and contractors) to take the initial security and privacy awareness training annually. Non-operational personnel, anyone that is involved in development and quality assurance, are also required to take the mandatory training. In addition, training related to the system being accessed, along with associated procedures, may be required. Security training is also required when there is a significant change to the system environment. |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 provides basic security and privacy awareness training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users. This is accomplished by requiring all staff to take a New Employee Orientation (NEO) security awareness training course, Standards of Business Conduct, within the first 30 days of their employment or transfer into the organization. This training course is facilitated by Microsoft Information Technology (MSIT) and Corporate Security, and encompasses standard business security measures, basic information security, and user actions to maintain security and to respond to suspected security incidents.  In addition, all staff are required to take security and privacy awareness training annually after their initial training. Office 365 has implemented the security training control by requiring all new users (employees and contractors) to take the initial security and privacy awareness training annually. Non-operational personnel, anyone that is involved in development and quality assurance, are also required to take the mandatory training. In addition, training related to the system being accessed, along with associated procedures, may be required. Security training is also required when there is a significant change to the system environment. |
| Part c | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 has implemented the security training control by requiring all staff, including managers, senior executives, and contractors, to take security and privacy awareness training annually after their initial training. Non-operational personnel, anyone that is involved in development and quality assurance, are also required to take the mandatory training. In addition, training related to the system being accessed, along with associated procedures, may be required. |

#### AT-2 (2) Control Enhancement (M) (H)

The organization includes security awareness training on recognizing and reporting potential indicators of insider threat.

| AT-02(2) | Control Summary Information |
| --- | --- |
| Responsible Role: Customer Administrator, Office 365 Trust Program Manager, Program Manager | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AT-02(2) - What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility:**  All customers, including government and non-government customers, should provide security awareness training to their users that includes content related to recognizing and reporting potential indicators of insider threat.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT security awareness training includes content related to recognizing and reporting potential indicators of insider threat. |

### AT-3 Role-Based Security Training (L) (M) (H)

The organization provides role-based security training to personnel with assigned security roles and responsibilities:

1. Before authorizing access to the information system or performing assigned duties;
2. When required by information system changes; and
3. [FedRAMP Assignment: at least annually] thereafter.

| AT-3 | Control Summary Information |
| --- | --- |
| Responsible Role: Customer Administrator, Office 365 Trust Program Manager, Program Manager | |
| Parameter AT-03(c):  annually or as needed based on changes to system or role and responsibility | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AT-3 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility:**  All customers, including government and non-government customers, are responsible for providing role-based training to their employees and vendors as necessary, including training on basic security awareness training and role-based training, as appropriate per job description. This training shall include requirements that customer users not bypass Office 365 security through actions such as:  1. Improperly forwarding documentation through Exchange Online  2. Improperly securing documentation hosted in SharePoint Online  3. Circumventing, disabling, or downgrading session-level encryption.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT provides role-based security-related training before authorizing access to the system or performing assigned duties. All Office 365 MT personnel are required to take the Microsoft System Administrator role-based training before being granted access to Office 365 MT. |
| Part b | **Customer Responsibility:**  All customers, including government and non-government customers, are responsible for providing role-based security training to their employees and vendors as necessary. This training shall include requirements that customer users not bypass Office 365 security through actions such as:  1. Improperly forwarding documentation through Exchange Online  2. Improperly securing documentation hosted in SharePoint Online  3. Circumventing, disabling, or downgrading session-level encryption.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT provides role-based security-related training before authorizing access to the system or when required by information system changes. All Office 365 MT personnel are required to take the Microsoft System Administrator role-based training before being granted access to Office 365 MT. |
| Part c | **Customer Responsibility:**  All customers, including government and non-government customers, are responsible for providing role-based security training to their employees and vendors as necessary (at least annually for government customers relying on FedRAMP certification).  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT provides role-based security-related training when required by system changes and at least annually. The Microsoft System Administrator training is tracked in corporate training tools and personnel are required to retake it annually. |

### AT-4 Security Training Records (L) (M)

The organization:

1. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and
2. Retains individual training records for [FedRAMP Assignment: at least one year].

| AT-4 | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Trust Program Manager | |
| Parameter AT-04(b):  3 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AT-4 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT utilizes corporate training tools to document and monitor security training. The corporate training tools provide reports, which tracks who has taken the basic security awareness and specific information system training. Each employee has access to their own account, which includes courses taken and elective courses that are suggested. A report can be generated from this tool to show what courses were taken by a specific employee. |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT utilizes corporate training tools to retain employee training records for basic security awareness and specific information system security training for at least 3 years. |

* 1. Audit and Accountability (AU)

### AU-1 Audit and Accountability Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and
2. Reviews and updates the current:
   1. Audit and accountability policy [FedRAMP Assignment: at every 3 years]; and
   2. Audit and accountability procedures [FedRAMP Assignment: at least annually].

| AU-01 | Control Summary Information |
| --- | --- |
| Responsible Role: Customer Administrator, Office 365 Trust Program Manager | |
| Parameter AU-01(a)(1):  Service Engineer Operations, Program Manager, Developer, Tester, Office 365 Trust Program Manager, Office 365 Security Manager, BCM | |
| Parameter AU-01(a)(2):  Service Engineer Operations, Program Manager, Developer, Tester, Office 365 Trust Program Manager, Office 365 Security Manager, BCM | |
| Parameter AU-01(b)(1):  annually | |
| Parameter AU-01(b)(2):  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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AU-01 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility:**  Government customers are responsible for developing and maintaining appropriate Audit and Accountability policies that govern auditing activities for their organization and users.  **Part 1:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Information Security Policy provides the overarching security guidance for Office 365 MT. This document addresses the purpose, scope, roles, responsibilities, compliance requirements, and required coordination among the various Microsoft organizations providing some level of support for the security of Office 365 MT. The Office 365 Information Security Policy is distributed to personnel responsible for implementing audit and accountability policies via SharePoint.  **Part 2:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Information Security Policy contains policies that must be met in the delivery and operation of Office 365 MT. Standards and Procedures to facilitate execution of these policies are documented in the Active Framework Controls, Office 365 Standard Operating Procedures (SOPs), and service team-specific SOPs. These standards and procedures act as adjuncts to the security policy and provide implementation level requirements and details to carry out specific operational tasks. A detailed mapping of Office 365 Standards and Procedures to each control is available. Office 365 SOPs are distributed to roles providing support for audit and accountability via SharePoint. |
| Part b | **Customer Responsibility:**  Government customers are responsible for developing and maintaining appropriate Audit and Accountability policies that govern auditing activities for their organization and users.  **Part 1:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Information Security Policy is reviewed and updated annually.  **Part 2:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Standard Operating Procedures (SOPs) are reviewed and updated annually. |

### AU-2 Audit Events (L) (M) (H)

The organization:

1. Determines that the information system is capable of auditing the following events: [FedRAMP Assignment: [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];
2. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events;
3. Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and
4. Determines that the following events are to be audited within the information system: [FedRAMP Assignment: organization-defined subset of the auditable events defined in AU-2 a. to be audited continually for each identified event].

AU-2 Additional FedRAMP Requirements and Guidance:

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

| AU-02 | Control Summary Information |
| --- | --- |
| Responsible Role: Customer Administrator, Office 365 Security Manager, Office 365 Trust Program Manager, Service Engineer Operations | |
| Parameter AU-02(a):  events specified by the Office 365 Security team | |
| Parameter AU-02(d):  events specified by the Office 365 Security 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AU-02 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility:**  Non-government customers not using ADFS do not have responsibility to produce audit records for Office 365 MT.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Security team has developed a general set of auditable events specific to the Office 365 MT Support based on ongoing risk assessments of the system which incorporate identified vulnerabilities, business requirements, and Office 365 MT Security standards. The Office 365 Security team specifies each event that must be audited for all servers.  Office 365 MT is capable of auditing these events on devices within the boundary.  For teams on PilotFish or Azure PaaS, The Azure Cyber Defense Operations Center (CDOC) team has developed a general set of auditable events which incorporates identified vulnerabilities, business requirements, and security standards. |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 Security incorporates business requirements from Office 365 MT as a whole and coordinates security audit functions from individual service teams to enhance mutual support and to help guide the selection of auditable events. |
| Part c | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Security team documents investigation procedures for each event. Office 365 Security has determined that the general and server-role event sets are adequate to support after-the-fact investigations.  For teams on PilotFish or Azure PaaS, The Azure Cyber Defense Operations Center (CDOC) team has developed a general set of auditable events which incorporates identified vulnerabilities, business requirements, and security standards. |
| Part d | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Security team specifies each event that must be audited for all servers. Events are audited continually.  For teams on PilotFish or Azure PaaS, The Azure Cyber Defense Operations Center (CDOC) team has developed a general set of auditable events which incorporates identified vulnerabilities, business requirements, and security standards. Events are audited continually. |

#### AU-2 (3) Control Enhancement (M) (H)

The organization reviews and updates the audited events [FedRAMP Assignment: annually or whenever there is a change in the threat environment].

AU-2 (3) Additional FedRAMP Requirements and Guidance:

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

| AU-02(3) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager, Office 365 Trust Program Manager, Service Engineer Operations | |
| Parameter AU-02(3):  annually or whenever there is a change in the threat 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AU-02(3) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The list of auditable events is maintained and reviewed at least annually by Office 365 Security team. For application-specific events, reviews and updates are considered at service reviews, or in the planning phases of feature milestones. Additionally, the list will be reviewed and updated whenever changes in the threat environment are communicated to Office 365 MT by the JAB.  For teams on PilotFish or Azure PaaS, the list of auditable events is maintained and reviewed at least annually by the Azure Cyber Defense Operations Center (CDOC) and updated by PilotFish deployment as needed. For application-specific events, reviews and updates are considered at service reviews, or in the planning phases of feature milestones. Additionally, the list will be reviewed and updated whenever changes in the threat environment are communicated to Azure by the JAB. |

### AU-3 Content of Audit Records (L) (M) (H)

The information system generates audit records containing information that establishes 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 individuals or subjects associated with the event.

| AU-03 | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager, Office 365 Trust Program Manager, 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AU-03 - What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility:**  Government and non-government customers using ADFS are responsible for auditing account creation, modification, disabling, and deletion events for their Active Directory infrastructure as these events also pertain to Office 365 MT access. For these events, these customers are responsible for capturing what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event. Customers using Windows servers to support their ADFS infrastructure automatically meet this requirement as Windows captures these event details by default. For more information regarding Windows event logging, see the following link: http://technet.microsoft.com/en-us/library/cc765981.aspx  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Per the Office 365 Security team, auditable events are required to contain the following information at a minimum to establish what events occurred, the sources of the events, and the outcomes of the events:  • Source User ID  • Target User ID – as relevant/appropriate for event type  • Event timestamp (Date & Time)  • Event details  o Type  o Outcome (success/failure)  o Detail information – defined per event type  • Source & Target Hostname – as relevant/appropriate for event type  • Source & Target network addresses and protocols – as relevant/appropriate for event type  This information is sufficient to identify the event type, source, location, outcome, time and the entity associated with the event (device or user). All auditable events captured in the Windows event log contain the minimum information required and in many cases additional information is captured. Office 365 MT does not filter any of the content generated. |

#### AU-3 (1) Control Enhancement (M)

The information system generates audit records containing the following additional information: [Assignment: organization-defined additional, more detailed information].

AU-3 (1) Additional FedRAMP Requirements and Guidance:

Requirement: The service provider defines audit record types [FedRAMP Assignment: 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]. The audit record types are approved and accepted by the JAB.

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-03(1) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager, Office 365 Trust Program Manager, Service Engineer Operations | |
| Parameter AU-03(1):  user ID; dates, times, and details of key events; terminal identity or location; records of successful and rejected system access attempts; records of successful and rejected data and their resource access attempts; changes to system configuration; use of privileges; use of system utilities and applications; files accessed and the kind of access; network addresses and protocols; alarms raised by the access control system; activation and deactivation of protection systems; success or failure indication; FedRAMP: session, connection, transaction or activity | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AU-03(1) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT generates audit records containing sufficient information to establish the type of event that occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any user/subject associated with the event. Office 365 MT Windows servers are configured to utilize the following fields:  • Source User ID  • Target User ID – as relevant/appropriate for event type  • Event timestamp (Date & Time)  • Event details  o Type  o Outcome (success/failure)  o Detail information – defined per event type  • Source & Target Hostname – as relevant/appropriate for event type  • Source & Target network addresses and protocols – as relevant/appropriate for event type |

### AU-4 Audit Storage Capacity (L) (M) (H)

The organization allocates audit record storage capacity in accordance with [Assignment: organization-defined audit record storage requirements].

| AU-04 | Control Summary Information |
| --- | --- |
| Responsible Role: Service Engineer Operations | |
| Parameter AU-04:  ability to retain at least 1-year worth of logs | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AU-04 - What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility:**  Government and non-government customers using ADFS are responsible for auditing account creation, modification, disabling, and deletion events for their Active Directory infrastructure as these events also pertain to Office 365 MT access. For these events, these customers are responsible for allocating audit record storage capacity and configuring auditing to reduce the likelihood of such capacity being exceeded. For more information regarding configuring event logging in Windows, including setting the maximum log size, see the following link: http://technet.microsoft.com/en-us/library/cc766178.aspx  Non-government customers not using ADFS do not have responsibility to produce audit records for Office 365 MT.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 utilizes a repository service to store audit information. The repository service dynamically allocates audit storage space to Office 365 MT. If Office 365 MT nears the limits of the storage capacity currently allocated, additional space in is assigned; the likelihood of audit storage capacity being exceeded is reduced by this dynamic model where allocated audit storage capacity grows with need. The repository service keeps at minimum ten petabytes free at any given time for dynamic allocation.  Azure is responsible for managing all network device logs. Azure implements audit storage capacity through a capacity planning procedure of both processing and storage requirements to ensure adequate resources are available for Azure. Due to the high volume of events received on servers and network devices, Azure audit collection settings are to overwrite when capacity is exceeded. Azure currently defines baseline requirements for local security audit log storage capacity to a window of at least 10 minutes of events on even Azure' most-active hosts. Events are continuously sent to the Syslog and Windows Event Collector, which are monitored by the Azure C+E Security Engineering Team, that have adequate storage capacity to handle the volume of events captured. In addition, collector data is archived via the event archive process for Syslog and Windows Event Collector, which are maintained for 180 days. In the event of an audit failure or audit storage capacity being reached, monitoring tools generate near-real time alerts to the C+E Security Engineering team, who are assigned to address the processing failure. |

### AU-5 Response to Audit Processing Failures (L) (M) (H)

The information system:

1. Alerts [Assignment: organization-defined personnel or roles] in the event of an audit processing failure; and
2. Takes the following additional actions: [FedRAMP Assignment: organization-defined actions to be taken; (overwrite oldest record)].

| AU-05 | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager, Office 365 Trust Program Manager, Service Engineer Operations | |
| Parameter AU-05(a):  Service Engineer Operations personnel, Office 365 Security Manager if confirmed | |
| Parameter AU-05(b):  moderate impact: overwrite oldest record | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AU-05 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility:**  Government and non-government customers using ADFS are responsible for auditing account creation, modification, disabling, and deletion events for their Active Directory infrastructure as these events also pertain to Office 365 MT access. For these events, these customers are responsible for alerting designated organizational officials in the event of an audit processing failure.  Non-government customers not using ADFS do not have responsibility to produce audit records for Office 365 MT.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Service teams use monitoring agents to verify that audit logs are being generated by systems and uploaded to a repository service. Audit processing failures generate alerts that are reported to Service Engineer Operations personnel and escalated to Office 365 Security as appropriate.  If Office 365 MT support nears the limits of the storage capacity currently allocated, additional space in assigned and the appropriate service team is alerted of the issue. |
| Part b | **Customer Responsibility:**  Government and non-government customers using ADFS are responsible for auditing account creation, modification, disabling, and deletion events for their Active Directory infrastructure as these events also pertain to Office 365 MT access. For these events, these customers are responsible for defining actions to be taken, in compliance with organizational policy, in the event of an audit processing failure. For more information regarding configuring log retention policy in Windows, see the following link: http://technet.microsoft.com/en-us/library/cc721981.aspx. For more information regarding shutting down the system in the event of an audit logging failure, see the following link: http://technet.microsoft.com/en-us/library/dd772720(v=WS.10).aspx  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  All audit logs are retained in a repository service. In the event of an audit processing failure, the oldest records are overwritten. |

### AU-6 Audit Review, Analysis, and Reporting (L) (M) (H)

The organization:

1. Reviews and analyzes information system audit records [FedRAMP Assignment: at least weekly] for indications of [Assignment: organization-defined inappropriate or unusual activity]; and
2. Reports findings to [Assignment: organization-defined personnel or roles].

AU-6 Additional FedRAMP Requirements and Guidance:

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

| AU-06 | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager, Office 365 Trust Program Manager, Service Engineer Operations | |
| Parameter AU-06(a):  1. weekly; 2. compromise identified in the Incident Response Plan | |
| Parameter AU-06(b):  Office 365 Security Manager | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AU-06 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility:**  Government and non-government customers using ADFS are responsible for auditing account creation, modification, disabling, and deletion events for their Active Directory infrastructure as these events also pertain to Office 365 MT access. For these events, these customers are responsible for reviewing and analyzing information system audit records for indications of inappropriate or unusual activity (at least weekly for FedRAMP compliance), and for reporting findings to designated organizational officials.  Non-government customers not using ADFS do not have responsibility to produce audit records for Office 365 MT.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Audit logs are uploaded to a repository service from all servers in the Office 365 MT environment. Each service team receives real time alerting on security events through various alerting tools and reports can be generated from the alerts and from the uploader service. Each team is responsible for reviewing and analyzing the alerts for indications of inappropriate or unusual activity, including indications of compromise. Findings are reported and escalated using standard security incident management channels: Tickets are opened to track these security incidents using ticket tracking software and the Office 365 Security team is engaged when appropriate. |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Service teams report and escalate findings by opening ticketing tool bugs and engaging the Office 365 Security team, who in turn follows the process defined in the Office 365 Security Incident Response Plan. |

#### AU-6 (1) Control Enhancement (M) (H)

The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.

| AU-06(1) | Control Summary Information |
| --- | --- |
| Responsible Role: Customer Administrator, Office 365 Security Manager, Office 365 Trust Program Manager, 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AU-06(1) - What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility:**  Government and non-government customers using ADFS are responsible for auditing account creation, modification, disabling, and deletion events for their Active Directory infrastructure as these events also pertain to Office 365 MT access. For these events, these customers are responsible for utilizing automated tools for integrating audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.  Non-government customers not using ADFS do not have responsibility to product audit records for Office 365 MT.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 Security uses an automated security alerting tools to review the audit logs, and to analyze the audit logs. Each service team also receives Near Real Time (NRT) alerting on security events through various NRT Security Monitoring alerting tools (different systems implemented by service teams e.g.: Vanquish; Arcsight; Azure Security Pack). Reports can be generated from the alerting tools and from the uploader service. Office 365 Security manages both audit monitoring and incident response. The primary objective of the audit monitoring process is to support incident response.  Teams using PilotFish use K9 as an automated mechanism to review and analyze audit logs. K9 also provides Near Real Time (NRT) alerting on security events. Reports can be generated from the alerts and from the uploader service. The Azure Cyber Defense Operations Center (CDOC) manages both audit monitoring and incident response for teams using PilotFish. The primary objective of the audit monitoring process is to support incident response. |

#### AU-6 (3) Control Enhancement (M) (H)

The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.

| AU-06(3) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager, Office 365 Trust Program Manager, 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AU-06(3) - What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility:**  Government and non-government customers using ADFS are responsible for auditing account creation, modification, disabling, and deletion events for their Active Directory infrastructure as these events also pertain to Office 365 MT access. For these events, these customers are responsible for analyzing and correlating audit records across different repositories to gain organization-wide situational awareness.  Non-government customers not using ADFS do not have responsibility to produce audit records for Office 365 MT.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Security Incident Management (SIM) team continuously correlates log files across multiple Office 365 MT systems using automated analytics tools. Audit logs are uploaded to a repository service from all servers in the Office 365 MT environment. Office 365 Security then uses automated security alerting tools to analyze the audit logs and generate actionable reports that the service teams can use to correct vulnerabilities and improve any weaknesses found.  The automated security alerting tools also look for issues that may be affecting multiple service teams, which allows Office 365 Security to gain organization-wide situational awareness and respond accordingly. |

### AU-7 Audit Reduction and Report Generation (M) (H)

The information system provides an audit reduction and report generation capability that:

1. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and
2. Does not alter the original content or time ordering of audit records.

| AU-07 | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager, Office 365 Trust Program Manager, 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AU-07 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility:**  Government and non-government customers using ADFS are responsible for auditing account creation, modification, disabling, and deletion events for their Active Directory infrastructure as these events also pertain to Office 365 MT access. For these events, these customers are responsible for providing an audit reduction and report generation capability that supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents.  Non-government customers not using ADFS do not have responsibility to produce audit records for Office 365 MT.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Audit logs are uploaded to a repository service from all servers in the Office 365 MT environment. Each service team receives NRT Security Monitoring alerting on security events through various alerting tools, and reports can be generated from the alerts and from the uploader service to support after-the-fact investigations of security incidents, to correct vulnerabilities, and to address any weaknesses found. |
| Part b | **Customer Responsibility:**  Government and non-government customers using ADFS are responsible for auditing account creation, modification, disabling, and deletion events for their Active Directory infrastructure as these events also pertain to Office 365 MT access. For these events, these customers are responsible for utilizing audit processing tools that do not change the original audit records or time ordering.  Non-government customers not using ADFS do not have responsibility to produce audit records for Office 365 MT.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The tools used in Office 365 MT to collect and process audit records do not permanently or irreversibly alter the original audit record content or time ordering. Office 365 MT scrubs logs of customer content before sending logs to the repository service. Specifically, scrubbing takes fields containing customer content, hashes that data, and replaces the field with the hash value. The rewritten log is sent to the repository service, while each service team stores a mapping of hash keys to hashes within the Office 365 MT accreditation boundary. The uploader service can then correlate, alert, and report on these anonymized hashes. If an alert or report requires investigation, the logs are imported back inside the boundary. The service team can then repopulate the logs to their original state using the hash to key mapping. |

#### AU-7 (1) Control Enhancement (M) (H)

The information system provides the capability to process audit records for events of interest based on [Assignment: organization-defined audit fields within audit records].

| AU-07(1) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager, Office 365 Trust Program Manager, Service Engineer Operations | |
| Parameter AU-07(1):  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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AU-07(1) - What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility:**  Government and non-government customers using ADFS are responsible for auditing account creation, modification, disabling, and deletion events for their Active Directory infrastructure as these events also pertain to Office 365 MT access. For these events, these customers are responsible for providing the capability to automatically process audit records for events of interest based on selectable event criteria.  Non-government customers not using ADFS do not have responsibility to produce audit records for Office 365 MT.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Logs are uploaded to a repository service, where they are aggregated, correlated, duplicated, and reduced into security or service-relevant alerts and alarms that are used by the service teams to analyze and respond appropriately to suspicious activity. Authorized personnel are able to perform database queries to process audit records for events of interest based on any fields contained within the records; authorized personnel are also able to generate reports that are used to review events of interest or investigate specific activities. |

### AU-8 Time Stamps (L) (M) (H)

The information system:

1. Uses internal system clocks to generate time stamps for audit records; and
2. Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets [Assignment: one second granularity of time measurement].

| AU-08 | Control Summary Information |
| --- | --- |
| Responsible Role: Azure, Service Engineer Operations | |
| Parameter AU-08(b):  one second precision | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AU-08 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility:**  Government and non-government customers using ADFS are responsible for auditing account creation, modification, disabling, and deletion events for their Active Directory infrastructure as these events also pertain to Office 365 MT access. For these events, these customers are responsible for using internal system clocks to generate time stamps for audit records; by default, Windows uses the internal system clock to generate time stamps for audit records, and this setting is not configurable.  Non-government customers not using ADFS do not have responsibility to produce audit records for Office 365 MT.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Audit records and events generated by Office 365 MT are logged with timestamps. Windows and Linux servers use the internal system clock to generate time stamps for audit records, and this setting is not configurable. |
| Part b | **Customer Responsibility:**  Government and non-government customers using ADFS are responsible for auditing account creation, modification, disabling, and deletion events for their Active Directory infrastructure as these events also pertain to Office 365 MT access. For these events, these customers are responsible for recording time stamps with audit records that can be mapped to UTC or GMT.  Non-government customers not using ADFS do not have responsibility to produce audit records for Office 365 MT.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT 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. Office 365 MT time stamps are precise at least to the second. |

#### AU-8 (1) Control Enhancement (M) (H)

The information system:

1. Compares the internal information system clocks with [FedRAMP Assignment: authoritative time source: [http://tf.nist.gov/tf-cgi/servers.cgi] [at least hourly]]; and
2. Synchronizes the internal system clocks to the authoritative time source when the time difference is greater than [Assignment: organization-defined time period].

| AU-08(1) | Control Summary Information |
| --- | --- |
| Responsible Role: Azure, Customer Administrator, Azure | |
| Parameter AU-08(1)(a):  1. at least hourly 2. http://tf.nist.gov/tf-cgi/servers.cgi | |
| Parameter AU-08(1)(b):  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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AU-08(1) - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility:**  Government and non-government customers using ADFS are responsible for auditing account creation, modification, disabling, and deletion events for their Active Directory infrastructure as these events also pertain to Office 365 MT access. For these events, these customers are responsible for synchronizing internal information system clocks at least hourly with http://tf.nist.gov/tf-cgi/servers.cgi in order to comply with FedRAMP requirements. For more information on configuring time sources in Windows, see the following link: http://technet.microsoft.com/en-us/library/cc794823(v=ws.10).aspx  Non-government customers not using ADFS do not have responsibility to produce audit records for Office 365 MT.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  All servers 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. Local domain controllers obtain their time updates from Azure time servers.  The Azure time servers are NTP Stratum 1 time servers that sync to Global Positioning System (GPS) satellites. Azure manages two different NTP time servers in separate geographic locations. The time servers are geographically dispersed and located in 2 separate Azure managed data centers in the CONUS. Azure chooses to use GPS satellites as the authoritative time source as an alternative to the Azure time hosts.  Teams using Linux hosts use the Azure Infrastructure time service.  Teams that rely on Azure inherit Internal system clock synchronization from Azure, which has a FedRAMP IaaS/PaaS P-ATO (package ID F1209051525). |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  All Office 365 MT servers synchronize the internal system clocks to the authoritative time source every hour and update the time if it is off by 1 millisecond or more. |

AU-8 (1) Additional FedRAMP Requirements and Guidance:

Requirement 1: 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 2: 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: The service provider selects primary and secondary time servers used by the NIST Internet time service, or by a Stratum-1 time server. The secondary server is selected from a different geographic region than the primary server.

If using Windows Active Directory, all servers should synchronize time with the time source for the Windows Domain Controller. If using some other directory services (e.g., LDAP), all servers should synchronize time with the time source for the directory server

| AU-08 (1) Req. | Control Summary Information |
| --- | --- |
| Responsible Role: Azure, Customer Administrator, 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AU-08 (1) Req. - What is the solution and how is it implemented? | |
| --- | --- |
| Req. 1 | **Customer Responsibility:**  Government and non-government customers using ADFS are responsible for auditing account creation, modification, disabling, and deletion events for their Active Directory infrastructure as these events also pertain to Office 365 MT access. For these events, these customers are responsible for synchronizing internal information system clocks to primary and secondary servers in different geographic regions.  Non-government customers not using ADFS do not have responsibility to produce audit records for Office 365 MT.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  All Windows servers 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. 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. Local domain controllers obtain their time updates from Azure time servers.  The Azure time servers are NTP Stratum 1-time servers that sync to Global Positioning System (GPS) satellites. 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 in the CONUS. Azure chooses to use GPS satellites as the authoritative time source as an alternative to the NIST time hosts.  Teams using Linux hosts use the Azure Infrastructure time service.  Teams that rely on Azure inherit Internal system clock synchronization from Azure, which has a FedRAMP IaaS/PaaS P-ATO (package ID F1209051525). |
| Req. 2 | **Customer Responsibility:**  Government and non-government customers using ADFS are responsible for auditing account creation, modification, disabling, and deletion events for their Active Directory infrastructure as these events also pertain to Office 365 MT access. For these events, these customers are responsible for synchronizing internal information system clocks on non-Windows systems to the Windows Server Domain Controller emulator or to the same time source for that server.  Non-government customers not using ADFS do not have responsibility to produce audit records for Office 365 MT.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  All Office 365 MT servers synchronize the internal system clocks to the authoritative time source every hour and update the time if it is off by 1 millisecond or more. |

### AU-9 Protection of Audit Information (L) (M) (H)

The information system protects audit information and audit tools from unauthorized access, modification, and deletion.

| AU-09 | Control Summary Information |
| --- | --- |
| Responsible Role: 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AU-9 - What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility:**  Government and non-government customers using ADFS are responsible for auditing account creation, modification, disabling, and deletion events for their Active Directory infrastructure as these events also pertain to Office 365 MT access. For these events, these customers are responsible for protecting audit information and audit tools from unauthorized access, modification, and deletion. For more information on controlling access in Windows, see the following link: http://technet.microsoft.com/en-us/library/hh831717.aspx  Non-government customers not using ADFS do not have responsibility to produce audit records for Office 365 MT.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Only Office 365 MT administrators have access to security logs. If an Office 365 MT administrator deletes log data locally, this activity is logged and an alert is generated.  In addition, all logs are uploaded to a repository service in near real time. EUII and customer content stored in the repository service is hashed or encrypted and can only be read when accessed through Office 365 MT by an authorized user. Authorized Office 365 MT personnel are only able to read information in the repository service and are not granted permissions to modify or delete logs. |

#### AU-9 (2) Control Enhancement (M) (H)

The information system backs up audit records [FedRAMP Assignment: at least weekly] onto a physically different system or system component than the system or component being audited.

| AU-09(2) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager, Office 365 Trust Program Manager, Service Engineer Operations | |
| Parameter AU-09(2):  at least weekly | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AU-09(2) - What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility:**  Government and non-government customers using ADFS are responsible for auditing account creation, modification, disabling, and deletion events for their Active Directory infrastructure as these events also pertain to Office 365 MT access. For these events, these customers are responsible for backing up audit records at least weekly onto a different system or media than the system being audited.  Non-government customers not using ADFS do not have responsibility to produce audit records for Office 365 MT.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Each Office 365 MT server uploads audit logs to a repository service, which is a system external to Office 365 MT, in near real time. In the event that real-time log shipping fails, logs are retained on the server until the connection is reinstated and they can be exported to the repository service. |

#### AU-9 (4) Control Enhancement (M) (H)

The organization authorizes access to management of audit functionality to only [Assignment: organization-defined subset of privileged users].

| AU-09(4) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager, Office 365 Trust Program Manager | |
| Parameter AU-09(4):  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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AU-09(4) - What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility:**  Government and non-government customers using ADFS are responsible for auditing account creation, modification, disabling, and deletion events for their Active Directory infrastructure as these events also pertain to Office 365 MT access. For these events, these customers are responsible for restricting access to only appropriate personnel.  Non-government customers not using ADFS do not have responsibility to produce audit records for Office 365 MT.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT restricts management of audit functionality within Office 365 MT to a limited subset of Service Engineer Operations personnel responsible for audit functionality. These personnel do not have the ability to modify or delete audit records from the repository service, and if they disable logging to the repository service, that action itself is logged. Repository service personnel do not have access to Office 365 MT. |

### AU-11 Audit Record Retention (M)

The organization retains audit records for [FedRAMP Assignment: at least ninety (90) days] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

AU-11 Additional FedRAMP Requirements and Guidance:

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

| AU-11 | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager, Office 365 Trust Program Manager | |
| Parameter AU-11:  at least 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AU-11 - What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility:**  Government and non-government customers using ADFS are responsible for auditing account creation, modification, disabling, and deletion events for their Active Directory infrastructure as these events also pertain to Office 365 MT access. For these events, these customers are responsible for retaining audit records for at least 90 days to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements. For more information on setting audit retention policy in Windows, see the following link: http://technet.microsoft.com/en-us/library/cc721981.aspx  Non-government customers not using ADFS do not have responsibility to produce audit records for Office 365 MT.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT retains audit records in a repository service for at least 90 days to support investigations of security incidents and to meet regulatory retention requirements. Customers are allowed to copy and store their own audit records to meet customer storage requirements. |

### AU-12 Audit Generation (L) (M) (H)

The information system:

1. Provides audit record generation capability for the auditable events defined in AU-2 a. at [FedRAMP Assignment: all information system components where audit capability is deployed/available];
2. Allows [Assignment: organization-defined personnel or roles] to select which auditable events are to be audited by specific components of the information system; and
3. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3.

| AU-12 | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager, Service Engineer Operations | |
| Parameter AU-12(a):  all information system components where audit capability is deployed | |
| Parameter AU-12(b):  Service Engineer Operations, Office 365 Security Manager | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| AU-12 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility:**  Government and non-government customers using ADFS are responsible for generating audit events for account creation, modification, disabling, and deletion activities for their Active Directory infrastructure as these events also pertain to Office 365 MT access. For more information on how to configure auditing of account management, see the following link: http://technet.microsoft.com/en-us/library/dd772693(v=WS.10).aspx  Non-government customers not using ADFS do not have responsibility to produce audit records for Office 365 MT.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT implements audit generation by configuring all system devices and servers to have the capability to generate audit records defined in AU-2 and AU-3. |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT implements audit generation by configuring all system network devices and servers to have the capability to generate audit records defined in AU-2 and AU-3.  Service teams configure audit generation for the operating system and the application layer to generate audit records as defined in AU-2 and AU-3.  Audit records are captured in a repository service, which allows for the record generation and reporting capabilities for the auditable events identified in AU-2 and AU-3. These capabilities also allow for the review of audit logs, should information contained within warrant a review. |
| Part c | **Customer Responsibility:**  Government and non-government customers using ADFS are responsible for generating audit events for account creation, modification, disabling, and deletion activities for their Active Directory infrastructure as these events also pertain to Office 365 MT access. Customers using Windows servers to support their ADFS infrastructure automatically meet this requirement as Windows captures these event details by default. For more information regarding Windows event logging, see the following link: http://technet.microsoft.com/en-us/library/cc765981.aspx  Non-government customers not using ADFS do not have responsibility to produce audit records for Office 365 MT.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Audit records are captured in active monitoring tools and stored in a repository service, which allows for the record generation and reporting capabilities for the auditable events identified in AU-2 with the content defined in AU-3. These capabilities also allow for the review of audit logs, should information contained within warrant a review. |

* 1. Security Assessment and Authorization (CA)

### CA-1 Certification, Authorization, Security Assessment Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls; and
2. Reviews and updates the current:
   1. Security assessment and authorization policy [FedRAMP Assignment: at least every three (3) years]; and
   2. Security assessment and authorization procedures [FedRAMP Assignment: at least annually].

| CA-01 | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Trust Program Manager | |
| Parameter CA-01(a)(1):  Service Engineer Operations, Program Manager, Developer, Tester, Office 365 Trust Program Manager, Office 365 Security Manager, BCM | |
| Parameter CA-01(a)(2):  Service Engineer Operations, Program Manager, Developer, Tester, Office 365 Trust Program Manager, Office 365 Security Manager, BCM | |
| Parameter CA-01(b)(1):  Annually | |
| Parameter CA-01(b)(2):  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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| CA-01 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Part 1:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Information Security Policy defines Office 365 MT policies. This document addresses the purpose, scope, roles, responsibilities, compliance requirements, and required coordination among the various Microsoft organizations providing some level of support for the security of Office 365 MT. Policies are made available to personnel responsible for implementing security assessment and authorization via SharePoint.  **Part 2:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Information Security Policy contains policies that must be met in the delivery and operation of Office 365 MT. Standards and procedures to facilitate execution of these policies are documented in the Active Framework Controls, Office 365 Standard Operating Procedures (SOPs), and service team-specific SOPs. These standards and procedures act as adjuncts to the security policy and provide implementation level requirements and details to carry out specific operational tasks. A detailed mapping of Office 365 Standards and Procedures to each control is available for review. Office 365 SOPs are distributed to roles providing support for security assessment and authorization controls via SharePoint. |
| Part b | **Part 1:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Information Security Policy is reviewed and updated annually by the Office 365 Trust team.  **Part 2:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Standard Operating Procedures (SOPs) are reviewed and updated annually. |

### CA-2 Security Assessments (L) (M) (H)

The organization:

1. Develops a security assessment plan that describes the scope of the assessment including:
   1. Security controls and control enhancements under assessment;
   2. Assessment procedures to be used to determine security control effectiveness; and
   3. Assessment environment, assessment team, and assessment roles and responsibilities;
2. Assesses the security controls in the information system and its environment of operation [FedRAMP Assignment: 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 requirements;
3. Produces a security assessment report that documents the results of the assessment; and
4. Provides the results of the security control assessment to [FedRAMP Assignment: individuals or roles to include the FedRAMP Program Management Office (PMO)].

| CA-02 | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Trust Program Manager | |
| Parameter CA-02(b):  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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| CA-02 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Part 1:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Security Assessment Plan (SAP) is developed by a 3PAO-certified independent assessor for Office 365 MT. Office 365 MT requires that the SAP include the security controls and enhancements under assessment, the assessment procedures, and an explanation of the assessment environment, team, and roles and responsibilities. The SAP is then reviewed and approved by Office 365 MT followed by a security assessment performed by the independent assessor. The SAP will be based on NIST SP 800-53A.  **Part 2:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  See part 1.  **Part 3:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  See part 1. |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT will assess security controls in the information system and its environment of operation each year. The controls will be assessed as part of the continuous monitoring process using a 3PAO-certified independent assessor as required. Other criteria, such as major system changes and changes in risk posture and vulnerabilities, will trigger assessments.  If an external system with which Office 365 MT maintains an interconnection has a FedRAMP P-ATO, Office 365 MT will leverage that P-ATO. Any system without a FedRAMP P-ATO from which security controls are inherited will be reviewed by the independent assessor with respect to security controls inherited from that system. |
| Part c | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT requires 3PAO-certified independent assessors to produce a Security Assessment Report (SAR) that 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. |
| Part d | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT provides the SAR to Authorizing Officials, together with the rest of the Authorization and Accreditation (A&A) package for an authorization decision. |

#### CA-2 (1) Control Enhancement (L) (M) (H)

The organization employs assessors or assessment teams with [Assignment: organization-defined level of independence] to conduct security control assessments.

CA-2 (1) Additional FedRAMP Requirements and Guidance:

Requirement: For JAB Authorization, must use an accredited Third Party Assessment Organization (3PAO).

| CA-02(1) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Trust Program Manager | |
| Parameter CA-02(1):  3PAO accreditation | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| CA-02(1) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Microsoft employs a FedRAMP-approved Third Party Assessment Organization (3PAO) as an independent assessor to conduct a security control assessment of Office 365 MT and its components. |

#### CA-2 (2) Control Enhancement (M) (H)

The organization includes as part of security control assessments, [FedRAMP Assignment: at least annually], [Selection: announced; unannounced], [Selection (one or more): in-depth monitoring; vulnerability scanning; malicious user testing; insider threat assessment; performance/load testing; [Assignment: organization-defined other forms of security assessment]].

CA-2 (2) Additional FedRAMP Requirements and Guidance:

Requirement: To include 'announced', 'vulnerability scanning’ to occur at least annually.

| CA-02(2) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Trust Program Manager | |
| Parameter CA-02(2):  1. annually; 2. announced; 3. in-depth monitoring, vulnerability scanning, malicious user testing through Red Team exercises, insider threat assessment, performance/load testing | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| CA-02(2) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Security team performs announced security control assessments at least annually. These assessments include in-depth monitoring, vulnerability scanning, insider threat assessment, malicious user testing through Red Team exercises, and performance/load testing. |

#### CA-2 (3) Control Enhancement (M) (H)

The organization accepts the results of an assessment of [FedRAMP Assignment: organization-defined information system] performed by [FedRAMP Assignment: any FedRAMP Accredited 3PAO] when the assessment meets [FedRAMP Assignment: the conditions of the JAB/AO in the FedRAMP Repository].

| CA-02(3) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Trust Program Manager | |
| Parameter CA-02(3):  1. the Office 365 information system; 2. any 3PAO; 3. the conditions of a P-ATO in the FedRAMP Secure 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| CA-02(3) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT will accept the results of an assessment of Office 365 MT performed by a 3PAO when that assessment meets the conditions of a P-ATO in the FedRAMP Secure Repository. |

### CA-3 System Interconnections (L) (M) (H)

The organization:

1. Authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements;
2. Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and
3. Reviews and updates Interconnection Security Agreements [FedRAMP Assignment: at least annually and on input from FedRAMP].

Table 13‑3 CA-3 Authorized Connections

| Authorized Connections Information System Name | Name of Organization System Connects To | Role and Name of Person Who Signed Connection Agreement | Name and Date of Interconnection Agreement |
| --- | --- | --- | --- |
| Microsoft Core Services Engineering | Microsoft | CSE Sr. Director, Operations Risk Management, Lisa Reshaur | Office 365 ISA with MSIT CorpNet,  03/19/2018 |
| MSIT (also known as CorpNet) is the Microsoft corporate network. MSIT contains services run on Microsoft’s  corporate network, not dedicated to Office 365 MT, such as source code repositories, system documentation repositories, and change ticketing. These services are secured via ISA with MSIT. | | | |
| Azure | Microsoft | Azure ISSO  Roger Chiou | Office 365 ISA with Azure and Azure Government, 07/31/2018 |
| Azure is an Infrastructure as a Service and Platform as a Service Cloud Computing Solution operated by Microsoft. Azure contains services run by Azure which are not dedicated to Office 365 MT. These services are used by AAD, as well as other service teams, to provide various aspects of the Office 365 Service. Azure also provides datacenter and network infrastructure, services and security. The use of Azure is covered via ISA. | | | |
| Cosmos | Microsoft | Cosmos Partner Director of PM, Ryan Waite | Office 365 and Cosmos ISA, 06/07/2018 |
| Cosmos is a service, not dedicated to Office 365 MT, that stores and reports on Office 365 MT log data. Office 365 MT scrubs logs  of customer content before sending logs to Cosmos. This connection is protected via ISA with Cosmos. | | | |
| Office 365 Support | Microsoft | O365 Support Authorizing Official  Elisabeth Zornes | Office 365 MT and Office 365 Support ISA, 06/07/2018 |
| Office 365 Support contains portals (not dedicated to Office 365 MT) used by Office 365 MT customer admins and Microsoft support representatives and secured via ISA with O365 Support. | | | |
| Global Traffic Management (GTM), HTTP Content  Delivery, HTTPS/TLS Content Delivery | Akamai | Vice President, Public Sector Tom Ruff | Office 365 and Akamai MOU, 03/19/2018 |
| Akamai represents services run by Akamai Corporation on behalf of Office 365 MT. These services include hosting some DNS records as well as hosting some static web content for enhanced availability. This use is protected via MOU with Akamai. | | | |
| Universal Store | Microsoft | Universal Store, Director of Compliance, Doug Taylor | Office 365 MT and Universal Store ISA, 03/19/2018 |
| Universal Store manages direct customer communication and billing for Office 365. AAD pushes  information to commerce to facilitate billing and marketing for commercial clients. Federal clients are billed  through a separate process and are not directly marketed to by Universal Store; federal customer  information is scrubbed by the Universal Store data collection process. | | | |

| CA-03 | Control Summary Information |
| --- | --- |
| Responsible Role: Customer Administrator, Office 365 Trust Program Manager | |
| Parameter CA-03(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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| CA-03 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT authorizes connections from the information system to other information systems outside of the authorization boundary through the use of vendor agreements, Memoranda of Understanding (MOU), Interconnection Security Agreements (ISA), and/or Service Level Agreements (SLA).  Microsoft has developed the necessary vendor agreements, MOUs, ISAs, SLA that document connections outside of the Federal authorization boundary. An ISA between Microsoft and customer will be developed if deemed necessary by the customer. |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 Trust is responsible for developing and maintaining MOU/ISA/SLA documents for Office 365 MT. These documents include the interface characteristics, security requirements and the nature of the information being communicated with third parties. |
| Part c | **Customer Responsibility:**  All customers, including government and non-government customers, are responsible for implementing security controls for information systems used to access the services provided by Office 365 MT.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT monitors its Interconnection Security Agreements (ISAs) to verify security requirements and conducts annual meetings with third parties to review agreements and any changes. Office 365 MT ensures that connection data described in ISAs is logged and monitored as part of the continuous monitoring process. Office 365 MT will also review ISAs as needed, based on input from FedRAMP, and update them when necessary. |

#### CA-3 (3) Control Enhancement (M) (H)

The organization prohibits the direct connection of an [Assignment: organization-defined unclassified, non-national security system] to an external network without the use of [FedRAMP Assignment: boundary protections which meet Trusted Internet Connection (TIC) requirements].

CA-3 (3) Additional FedRAMP Requirements and Guidance: Refer to Appendix H – Cloud Considerations of the TIC 2.0 Reference Architecture document. Link: https://www.fedramp.gov/files/2015/04/TIC\_Ref\_Arch\_v2-0\_2013.pdf

| CA-03(3) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Trust Program Manager | |
| Parameter CA-03(3):  1. Office 365 information system; 2. organization defined boundary protection 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| CA-03(3) - What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility:**  Customers are responsible for routing their internet traffic through a TIC. This can be accomplished by restricting access to the government customer’s ADFS to only traffic originating on the government customer’s internal network. This will force government customers attempting to connect to Office 365 MT to VPN into the customer’s network or directly be on the network at the time of authentication. If the government customer has implemented a TIC on their network, traffic to Office 365 MT will then be routed through this TIC. For more information, see the following TechNet article: http://technet.microsoft.com/en-us/library/hh526961(v=ws.10).aspx  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  All Office 365 MT systems connect to external networks only through managed boundary protection devices (i.e. routers, firewalls). |

#### CA-3 (5) Control Enhancement (M)

The organization employs [Selection: allow-all, deny-by-exception, deny-all, permit by exception] policy for allowing [Assignment: organization-defined information systems] to connect to external information systems.

CA-3 (5) Additional FedRAMP Requirements and Guidance:

Guidance: For JAB Authorization, CSPs shall include details of this control in their Architecture Briefing

| CA-03(5) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Trust Program Manager | |
| Parameter CA-03(5):  1. deny-all, permit by exception; 2. all information systems within the system 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| CA-03(5) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT employs a deny-all, permit-by-exception policy for allowing the Office 365 MT information system to connect to external information systems. |

### CA-5 Plan of Action and Milestones (L) (M) (H)

The organization:

1. Develops a plan of action and milestones for the information system to document the organization’s planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and
2. Updates existing plan of action and milestones [FedRAMP Assignment: at least monthly] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

CA-5 Additional FedRAMP Requirements and Guidance:

Requirement: Plan Of Action & Milestones (POA&M)s must be provided at least monthly.

| CA-05 | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Trust Program Manager | |
| Parameter CA-05(b):  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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| CA-05 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Trust team develops Plans of Action and Milestones (POA&Ms) in accordance with OMB guidance and FedRAMP requirements. POA&Ms are developed and maintained by Office 365 Trust. They are recorded in ticket tracking tools to ensure an auditable record of each POA&M.  Additionally, they are exported into the FedRAMP POA&M template monthly. The POA&Ms describe how the information system owner intends to address the vulnerabilities and risks (i.e. risk acceptance, risk mitigation, risk avoidance, risk transference). |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 Trust updates the POA&Ms which include a list of the vulnerabilities and risks discovered during Authorization and Accreditation (A&A) activities and security control monitoring on a monthly basis as part of the Office 365 MT Continuous Monitoring process. |

### CA-6 Security Authorization (L) (M) (H)

The organization:

1. Assigns a senior-level executive or manager as the authorizing official for the information system;
2. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and
3. Updates the security authorization [FedRAMP Assignment: in accordance with OMB A-130 requirements or when a significant change occurs].

CA-6c Additional FedRAMP Requirements and Guidance:

Guidance: Significant change is defined in NIST Special Publication 800-37 Revision 1, Appendix F ([SP 800-37](http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf)). 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-06 | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Trust Program Manager | |
| Parameter CA-06(c):  every 3 years or when there is a significant 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| CA-06 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  As part of the Authorization and Accreditation (A&A) process, a designated Authorizing Official (AO) will review the Microsoft A&A package to determine if vulnerabilities identified in the information system pose an acceptable level of risk to agency operations, assets, and individuals. |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Following the review of the accreditation package and consultation with key agency officials, the Authorizing Official (AO) will render an accreditation decision to authorize system operation. |
| Part c | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 MT Security Authorization package is updated every three years or when there is a significant change (as defined in NIST Special Publication 800-37 Revision 1, Appendix F). |

### CA-7 Continuous Monitoring (L) (M) (H)

The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes:

1. Establishment of [Assignment: organization-defined metrics] to be monitored;
2. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring;
3. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy;
4. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy;
5. Correlation and analysis of security-related information generated by assessments and monitoring;
6. Response actions to address results of the analysis of security-related information; and
7. Reporting the security status of organization and the information system to [FedRAMP Assignment: to meet Federal and FedRAMP requirements] [Assignment: organization-defined frequency].

CA-7 Additional FedRAMP Requirements and Guidance:

Requirement: Operating System Scans: at least monthly Database and Web Application Scans: at least monthly All scans performed by Independent Assessor: at least annually.

Guidance: CSPs must provide evidence of closure and remediation of a high vulnerability within the timeframe for standard POA&M updates.

| CA-07 | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Trust Program Manager | |
| Parameter CA-07(a):  rate of closure/remediation of POA&Ms and high vulnerabilities | |
| Parameter CA-07(b):  1. continuous; 2. Monthly | |
| Parameter CA-07(g):  1. Office 365 Management and authorized customers; 2. 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| CA-07 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT has established a continuous monitoring strategy and a continuous monitoring program, documented in the "Continuous Monitoring Strategy Guide". The PAVC team provides evidence of closure and remediation of high vulnerabilities on a monthly basis for Operating System Scans. |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT has established a continuous monitoring strategy and a continuous monitoring program, documented in the "Continuous Monitoring Strategy Guide". The PAVC team provides evidence of closure and remediation of high vulnerabilities on a monthly basis for BeyondTrust scans. |
| Part c | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT has established a continuous monitoring strategy and a continuous monitoring program, documented in the "Continuous Monitoring Strategy Guide". The PAVC team provides evidence of closure and remediation of high vulnerabilities on at least an annual basis for all scans performed by an Independent 3rd Party Assessor. |
| Part d | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  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 Office 365 MT Operational Service Readiness reviews. POA&M updates are provided to customers monthly, consistent with FedRAMP requirements. |
| Part e | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT has established a continuous monitoring strategy, documented in the "Continuous Monitoring Strategy Guide". This strategy is implemented by the Office 365 Continuous Monitoring team and includes correlation and analysis of security-related information generated by assessments and monitoring, including vulnerability scan results, POA&M updates, and recurring control testing. |
| Part f | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT has established a continuous monitoring strategy, documented in the "Continuous Monitoring Strategy Guide". This strategy is implemented by the Office 365 Continuous Monitoring team and includes response actions to address results of the analysis of security-related information, including vulnerability mitigation, POA&M resolution, and control gap closure. |
| Part g | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  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 Office 365 MT Operational Service Readiness reviews. POA&M updates are provided to customers and the JAB monthly, consistent with FedRAMP requirements. |

CA-07 Additional FedRAMP Requirements and Guidance:

Requirement 1: Operating System Scans: at least monthly

Requirement 2: Database and Web Application Scans: at least monthly

Requirement 3: All scans performed by Independent Assessor: at least annually

| CA-07 Req. | Control Summary Information |
| --- | --- |
| Responsible Role: Program Manager, Office 365 Trust Program Manager | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| CA-07 Req. - What is the solution and how is it implemented? | |
| --- | --- |
| Req. 1 | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Please see RA-5 and RA-5(5). |
| Req. 2 | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC**  Please see RA-5 and RA-5(5). |
| Req. 3 | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  As discussed in RA-05(9), Office 365 MT plans for 3PAO-conducted penetration testing to be carried out on an annual basis. |

#### CA-7 (1) Control Enhancement (M) (H)

The organization employs assessors or assessment teams with [Assignment: organization-defined level of independence] to monitor the security controls in the information system on an ongoing basis.

| CA-07(1) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Trust Program Manager | |
| Parameter CA-07(1):  Office 365 oversight responsibilities | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| CA-07(1) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 Trust monitors service team implementation of security controls on an ongoing basis in accordance with the "Continuous Monitoring Strategy Guide". In addition, 3PAOs review and validate continuous monitoring efforts as part of the Security Assessment Report (SAR). |

### CA-8 Penetration Testing (M) (H)

The organization conducts penetration testing [FedRAMP Assignment: at least annually] on [Assignment: organization-defined information systems or system components].

| CA-08 | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Trust Program Manager | |
| Parameter CA-08:  1. annually; 2. components of information system specified in the rules of engagement for a particular penetration test | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| CA-08 - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  As part of Office 365 MT's FedRAMP assessment by a 3PAO certified independent auditor, Office 365 MT will have the 3PAO perform penetration testing consistent with FedRAMP requirements. The penetration testing plan will be documented in the Security Assessment Plan (SAP) and results will be included in the Security Assessment Report (SAR).  Additionally, an independent penetration testing team within Microsoft’s security organization conducts annual unannounced penetration testing (tests may be coordinated with Office 365 MT management personnel in order to mitigate risk to the availability of Office 365 MT; Office 365 MT management personnel do not notify operational/technical personnel in these cases). |

#### CA-8 (1) Control Enhancement (M) (H)

The organization employs an independent penetration agent or penetration team to perform penetration testing on the information system or system components.

| CA-08(1) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Trust Program Manager | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| CA-08(1) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  As part of Office 365 MT's FedRAMP assessment by a 3PAO certified independent auditor, Office 365 MT will have the 3PAO perform penetration testing consistent with FedRAMP requirements. The penetration testing plan will be documented in the Security Assessment Plan (SAP) and results will be included in the Security Assessment Report (SAR). |

### CA-9 Internal System Connections (L) (M) (H)

The organization:

1. Authorizes internal connections of [Assignment: organization-defined information system components or classes of components] to the information system; and
2. Documents, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated.

| CA-9 | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Trust Program Manager | |
| Parameter CA-09(a):  servers within the Office 365 inventory, connections between 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| CA-9 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  All devices within the accreditation boundary are by definition authorized to connect to Office 365 MT. Service team administrators are authorized to connect to systems through the TSGs as described in AC-17. Customer users are authorized to connect through the public-facing components of the Office 365 MT service. |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Interface characteristics, security requirements, and nature of information being communicated is documented in the data flow diagram provided in Section 10 of this SSP. |

* 1. Configuration Management (CM)

### CM-1 Configuration Management Policies and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the configuration management policy and associated configuration management controls; and
2. Reviews and updates the current:
   1. Configuration management policy [FedRAMP Assignment: at least every three (3) years]; and
   2. Configuration management procedures [FedRAMP Assignment: at least annually].

| CM-1 | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Trust Program Manager | |
| Parameter CM-01(a)(1):  Service Engineer Operations, Program Manager, Developer, Tester, Office 365 Trust Program Manager, Office 365 Security Manager, BCM | |
| Parameter CM-01(a)(2):  Service Engineer Operations, Program Manager, Developer, Tester, Office 365 Trust Program Manager, Office 365 Security Manager, BCM | |
| Parameter CM-01(b)(1):  Annually | |
| Parameter CM-01(b)(2):  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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| CM-1 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility:**  Government customers are responsible for developing and maintaining appropriate Configuration Management policies that govern configuration management activities for their organization and users.  **Part 1:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Information Security Policy defines Office 365 MT policies. This document addresses the purpose, scope, roles, responsibilities, compliance requirements, and required coordination among the various Microsoft organizations providing some level of support for the security of Office 365 MT. Policies are distributed to personnel responsible for implementing configuration management policies and procedures via SharePoint.  **Part 2:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Standards and procedures to facilitate execution of these policies are documented in the Active Framework Controls, Office 365 Standard Operating Procedures (SOPs), and service team-specific SOPs. These standards and procedures act as adjuncts to the security policy and provide implementation level requirements and details to carry out specific operational tasks. A detailed mapping of Office 365 standards and procedures to each control is available for review. Office 365 SOPs are distributed via SharePoint. |
| Part b | **Customer Responsibility:**  Government customers are responsible for developing and maintaining appropriate Configuration Management policies that govern configuration management activities for their organization and users.  **Part 1:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Information Security Policy is reviewed and updated annually.  **Part 2:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Standard Operating Procedures (SOP) are reviewed and updated annually. |

### CM-2 Baseline Configuration (L) (M) (H)

The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.

| CM-02 | Control Summary Information |
| --- | --- |
| Responsible Role: Azure, 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| CM-02 - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT service teams develop, document, and maintain under configuration control, a current baseline OS configuration of their production systems.  DNS, SPO, SWE, and WAC inherit Azure IPAK images. Azure is responsible for developing, documenting and maintaining these images under configuration control.  EXO develops their own initial OS images and document, and maintain them under configuration control in version control tools.  IP uses EXO baseline configurations.  MA, OLM, OSI, and SUE inherit the Azure VM OS images. Azure is responsible for developing, documenting and maintaining under configuration control these images at least annually, as described in the Azure SSP.  SFB, SPO, and MSTeams apply baseline configurations using configuration scripts. These service teams develop, document, and maintain these configuration scripts under configuration control in version control tools.  OS baseline images are managed in PilotFish, which updates images and maintains them under configuration control. |

#### CM-2 (1) Control Enhancement (M)

The organization reviews and updates the baseline configuration of the information system:

1. [FedRAMP Assignment: at least annually];
2. When required due to [FedRAMP Assignment: to include when directed by the JAB]; and
3. As an integral part of information system component installations and upgrades.

| CM-2(1) | Control Summary Information |
| --- | --- |
| Responsible Role: Azure, Service Engineer Operations | |
| Parameter CM-02(1)(a):  at least annually | |
| Parameter CM-02(1)(b):  a significant 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| CM-2(1) - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT service teams review and update their baseline configurations at least annually and when there is a significant change. |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  See CM-02(1)(a) |
| Part c | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT reviews and updates the baseline configuration based on new security configurations or changes to existing security configurations. Any change made to baseline configurations are reviewed by the Azure Change Advisory Board (CAB) for IPAK baseline configurations, and the service teams for each of their own baseline configurations. |

#### CM-2 (2) Control Enhancement (M) (H)

The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.

| CM-02(2) | Control Summary Information |
| --- | --- |
| Responsible Role: Azure, 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| CM-02(2) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  IPAK images and VM OS images are provided by Azure. Azure is responsible for developing, documenting and maintaining under configuration control of these images as described in the Azure SSP. Version control and ticketing tools are used to manage the maintenance of OS images for at least 6 months to support rollback capability. |

#### CM-2 (3) Control Enhancement (M)

The organization retains [Assignment: organization-defined previous versions of baseline configurations of the information system] to support rollback.

| CM-02(3) | Control Summary Information |
| --- | --- |
| Responsible Role: Azure, Service Engineer Operations | |
| Parameter CM-02(3):  6 months of baseline configurations | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| CM-02(3) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  IPAK images and VM OS images are provided by Azure. Azure is responsible for developing, documenting and maintaining under configuration control of these images as described in the Azure SSP. Version control and ticketing tools are used to manage the maintenance of OS images for at least 6 months to support rollback capability. |

#### CM-2 (7) Control Enhancement (M) (H)

The organization:

1. Issues [Assignment: organization-defined information systems, system components, or devices] with [Assignment: organization-defined configurations] to individuals traveling to locations that the organization deems to be of significant risk; and
2. Applies [Assignment: organization-defined security safeguards] to the devices when the individuals return.

| CM-2(7) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Trust Program Manager | |
| Parameter CM-02(7)(a):  1. not applicable; 2. not applicable | |
| Parameter CM-02(7)(b):  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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869) | |

| CM-2(7) - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  In accordance with the Office 365 Data Handling Standard, customer content is never stored outside of Office 365 MT, which is physically located within the continental United States. Office 365 MT personnel do not travel with devices within the Office 365 MT inventory. As such, this control is not applicable. |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  See part a. |

### CM-3 Configuration Change Control (M) (H)

The organization:

1. Determines the types of changes to the information system that are configuration-controlled;
2. Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses;
3. Documents configuration change decisions associated with the information system;
4. Implements approved configuration-controlled changes to the information system;
5. Retains records of configuration-controlled changes to the information system for [Assignment: organization-defined time period];

CM-3 (e) Additional FedRAMP Requirements and Guidance:

Guidance: In accordance with record retention policies and procedures.

1. Audits and reviews activities associated with configuration-controlled changes to the information system; and
2. Coordinates and provides oversight for configuration change control activities through [FedRAMP Assignment: see additional FedRAMP requirements and guidance] that convenes [Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined configuration change conditions]].

CM-3 Additional FedRAMP Requirements and Guidance:

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.

| CM-3 | Control Summary Information |
| --- | --- |
| Responsible Role: Azure, Service Engineer Operations | |
| Parameter CM-03(e):  at least one year | |
| Parameter CM-03(g):  1. CAB 2. as needed 3. major 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869) | |

| CM-3 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT has defined the types of changes that must be configuration controlled: all changes to operational systems, other than security patches, can only be made after a security review and authorization through the change management process. This is documented in the Office 365 Configuration Management Plan. |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  All changes to the system under configuration control are reviewed, and approved or disapproved with explicit consideration for security impact analysis. The security impact analysis process is detailed in CM-4. |
| Part c | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Service teams use ticketing tools to document evidence of approval and track all changes. |
| Part d | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Ticketing tools ensure that configuration-controlled changes are implemented after they are approved by tracking the change through implementation. |
| Part e | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Service teams use ticketing tools to document evidence of approval and track all changes. These tools retain documentation of changes and change approval/disapproval for at least one year. |
| Part f | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Ticketing tools retain an audit history, showing what actions were taken and by whom, including approvals. Office 365 MT service teams review the audit history as required by investigations and during annual independent security assessments. |
| Part g | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Change Advisory Board (CAB) and its members are chartered to formally "Approve" or "Deny" all changes prior to implementation. Configuration and code changes follow a common system development process which includes provisions for oversight and approval. The CAB convenes as needed to support changes to the environment.  If a quorum for the CAB exists, the change process begins with a RFC, which documents:  • What is being changed  • Where the change is to be implemented  • Why the change is needed  • Change deployment steps  • What is the impact of doing and not doing the requested change  • Change mitigation (Plan B, C, D)  • When is the change desired to be implemented  • Change rollback criteria and instructions  Further details of the change management process are detailed in the service team-specific change management Standard Operating Procedures (SOP).  Any major changes to or developments of Office 365 MT that may affect its services to the federal government and associated service consumers will be communicated via the FedRAMP major change process. |

### CM-4 Security Impact Analysis (L) (M) (H)

The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.

| CM-04 | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager, 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| CM-04 - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Service teams are required by the Office 365 Configuration Management Plan to assess potential security impact of all changes when reviewing changes for approval. Service team personnel are trained to assess both security-related changes (changes to the configurable security-related parameters of Office 365 MT, registry settings, account, file, and directory settings (i.e., permissions), and settings for services, ports, protocols, and remote connections) as well as possible broader impact to security architecture. |

### CM-5 Access Restrictions for Change (M) (H)

The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.

| CM-05 | Control Summary Information |
| --- | --- |
| Responsible Role: Azure, Office 365 Security Manager, Program Manager | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| CM-05 - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT 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) and Azure Active Directory (AAD). All accounts created in support of Office 365 MT 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 undergone background checks and have gone through the approval process for Operations-level read access to production, used during critical incident escalations.  In EXO, IP, and SPO, common change processes are scripted in commandlets. These commandlets are checked-in and reviewed through the change management process. The ability to execute these commandlets is restricted to members of appropriate security groups, who can execute them via JIT elevations. System access to perform changes beyond the scope of these pre-approved commandlets is allowed for emergency situations through the use of RDP via TSGs.  Physical access control is inherited from Azure, which has a FedRAMP IaaS/PaaS P-ATO (package ID F1209051525). |

#### CM-5 (1) Control Enhancement (M) (H)

The information system enforces access restrictions and supports auditing of the enforcement actions.

| CM-05(1) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| CM-05(1) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Service teams use Active Directory (AD), Azure Active Directory (AAD), and JIT tooling to control access to change functions. AD and AAD defines the access that is available, and JIT tools provide time-limited permission elevation when users actually need to use that access. AD and JIT tools are automated, and actions taken (account creation, change, disabling, removal for AD; account elevation for JIT tools) are automatically audited.  Bing, EXO, IP, SPO, MSTeams, and OLM also use Torus, which only allows pre-approved changes to the information system. The ability to implement these pre-approved changes is access-restricted to the appropriate security groups. Any commandlet run in Torus is logged per auditing requirements defined by the security team. |

#### CM-5 (3) Control Enhancement (M) (H)

The information system prevents 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.

CM-5 (3) Additional FedRAMP Requirements and Guidance:

Guidance: If digital signatures/certificates are unavailable, alternative cryptographic integrity checks (hashes, self-signed certs, etc.) can be used.

| CM-05(3) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager, Program Manager, Service Engineer Operations | |
| Parameter CM-05(3):  any software or firmware components when the vendor provides digitally signed products | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| CM-05(3) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT has determined that solutions to fully meet this control pose unacceptable risks to system availability. A complete discussion of these risks and the mitigating controls in place are documented in “Guidance on FedRAMP Control CM-5(3)” Decision Log. |

#### CM-5 (5) Control Enhancement (M) (H)

The organization:

1. Limits privileges to change information system components and system-related information within a production or operational environment; and
2. Reviews and reevaluates privileges [FedRAMP Assignment: at least quarterly].

| CM-5 (5) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager, Program Manager | |
| Parameter CM-05(5)(b):  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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| CM-5 (5) - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Service teams restrict access to the production environment to approved members of specific security groups. By default, developers/integrators do not have permissions to change hardware/software/firmware in production. Such permissions can be granted for a short time as needed (such as when a developer/integrator is acting as On-Call Engineer), through Lockbox or another just-in-time elevation mechanism. |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Service teams review privileged access at least quarterly, consistent with normal account review processes. |

### CM-6 Configuration Settings (L) (M) (H)

The organization:

1. Establishes and documents configuration settings for information technology products employed within the information system using [FedRAMP Assignment: see CM-6(a) Additional FedRAMP Requirements and Guidance] that reflect the most restrictive mode consistent with operational requirements;

CM-6(a) Additional FedRAMP Requirements and Guidance:

Requirement 1: The service provider shall use the Center for Internet Security guidelines (Level 1) to establish configuration settings or establishes its own configuration settings if USGCB is not available. If no recognized USGCB is available for the technology in use, the CSP should create their own baseline and include a justification statement as to how they came up with the baseline configuration settings.

Requirement 2: The service provider shall ensure that checklists for configuration settings are Security Content Automation Protocol (SCAP) (http://scap.nist.gov/) validated or SCAP compatible (if validated checklists are not available).

Guidance: Information on the USGCB checklists can be found at: http://usgcb.nist.gov/usgcb\_faq.html#usgcbfaq\_usgcbfdcc.

Implements the configuration settings;

Identifies, documents, and approves any deviations from established configuration settings for [Assignment: organization-defined information system components] based on [Assignment: organization-defined operational requirements]; and

Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

| CM-6 | Control Summary Information |
| --- | --- |
| Responsible Role: Azure, Service Engineer Operations | |
| Parameter CM-06(a):  mandatory configuration settings from configuration baselines | |
| Parameter CM-06(c):  1. all information system components; 2. 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| CM-6 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Teams establish and document configuration settings as a part of establishing a baseline configuration and implementing configuration change control. Mandatory configuration settings are applied through the use of GPOs, setting of registry keys and use of configuration scripts. Input to these configuration settings and scripts comes from product architecture and security analysis as well as direction from Office 365 Security. CIS Benchmarks are used in the development of baseline configurations and configuration settings.  Configuration settings established as part of IPAK and VM OS images are inherited from Azure, which has a FedRAMP P-ATO (F1209051525).  **Planned:**  The Office 365 PAVC team is using Beyond Trust to perform scans for configuration settings. Beyond Trust scans against CIS Benchmarks settings in the system and reports on current status. The Office 365 PAVC team is building a process for making the CIS Benchmark scan data available to service teams to action on any gaps that may exist.  POA&M MT-0076 is tracking a project to granularly track and implement CIS Benchmark requirements within EXO, SFB, and SPO. |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT service team personnel use automated deployment mechanisms and documented standard operating procedures to implement the mandatory configuration settings for all servers, network devices, and applications. Automated deployment systems ensure that only the settings defined in part a of this control and approved as part of change management processes are deployed to production. |
| Part c | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  All components of the information system are configured based on their role; all components with the same role have the same configuration with no exceptions/deviations.  In the unlikely event that an exception/deviation is required, service teams would log configuration changes into ticketing tools and follow the regular change approval process. |
| Part d | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  All configuration changes are limited to the specific Office 365 MT personnel responsible for the component and are captured in audit logs. In addition, vulnerability scans are run on a weekly basis to assist in determining the effectiveness of the configuration settings on the applications and servers.  Only certain members of Office 365 MT Service Team Operations groups have the privileges to make changes to the configuration of the system. If an unauthorized person attempts to make changes, the system will automatically deny the request. The action will be captured in the audit logs and will be investigated. If further actions are required, it will be reported up to Office 365 Security or Azure (as appropriate) and service team incident response personnel will be notified immediately. The audit logs are maintained in storage for at least 90 days to support after-the-fact investigations.  A review process is in place to ensure that only approved changes are implemented. |

#### CM-6 (1) Control Enhancement (M) (H)

The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings for [Assignment: organization-defined information system components].

| CM-06(1) | Control Summary Information |
| --- | --- |
| Responsible Role: Azure, Service Engineer Operations | |
| Parameter CM-06(1):  network components, servers and virtual machines | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| CM-06(1) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 MT service teams use Active Directory Group Policy Objects (GPOs) as an automated mechanism to centrally manage, apply, and verify security configuration settings for servers and virtual machines.  Service teams using Azure rely on Azure to centrally provision machines and apply changes. These service teams use Source Depot and Azure Resource Manager as automated mechanisms to centrally manage, apply, and verify security configuration settings for Azure virtual machine images. Azure Resource Manager is an automated mechanism to centrally manage, apply, and verify security configuration settings for Azure virtual machine images. |

### CM-7 Least Functionality (L) (M) (H)

The organization:

1. Configures the information system to provide only essential capabilities; and
2. Prohibits or restricts the use of the following functions, ports, protocols, and/or services [FedRAMP Assignment: United States Government Configuration Baseline (USGCB)]

CM-7 Additional FedRAMP Requirements and Guidance:

Requirement: The service provider shall use the Center for Internet Security guidelines (Level 1) 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 USGCB is not available. If no recognized USGCB is available for the technology in use, the CSP should create their own baseline and include a justification statement as to how they came up with the baseline configuration settings.

Guidance: Information on the USGCB checklists can be found at: http://usgcb.nist.gov/usgcb\_faq.html#usgcbfaq\_usgcbfdcc

Partially derived from AC-17 (8).

| CM-7 | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager, Service Engineer Operations | |
| Parameter CM-07(b):  Office 365 Ports Protocols and Services Blacklist | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| CM-7 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT uses a combination of USGCB guidance and CIS Benchmarks for development of all base operating system images deployed within the system. These baselines help to ensure that only essential functions, ports, protocols, and services are enabled for each server role. |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT prohibits and restricts the use of specific ports, protocols, and services defined in the Office 365 MT Ports Protocols and Services Blacklist, which is integrated into the Office 365 MT change management process. |

#### CM-7 (1) Control Enhancement (M) (H)

The organization:

1. Reviews the information system [FedRAMP Assignment: at least Monthly] to identify unnecessary and/or nonsecure functions, ports, protocols, and services; and
2. Disables [Assignment: organization-defined functions, ports, protocols, and services within the information system deemed to be unnecessary and/or nonsecure].

| CM-7 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager, Service Engineer Operations | |
| Parameter CM-07(1)(a):  monthly | |
| Parameter CM-07(1)(b):  Office 365 Ports Protocols and Services Blacklist | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| CM-7 (1) - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT reviews Access Control Lists (ACLs) through PAVC security scans and a continuous monitoring tracking ticket at least monthly to identify ports and protocols that are no longer necessary to the system or are nonsecure. |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT disables specific ports, protocols, and services defined in the Office 365 MT Ports Protocols and Services Blacklist. |

#### CM-7 (2) Control Enhancement (M) (H)

The information system prevents program execution in accordance with [Selection (one or more): [Assignment: organization-defined policies regarding software program usage and restrictions]; rules authorizing the terms and conditions of software program usage].

CM-7(2) Additional FedRAMP Requirements and Guidance:

Guidance: 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., white listing). This control is not to be based off of strictly written policy on what is allowed or not allowed to run.

| CM-07(2) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Trust Program Manager | |
| Parameter CM-07(2):  the Office 365 Security Policy and supporting Active Framework security 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| CM-07(2) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT has determined that solutions to fully meet this control pose unacceptable risks to system availability. A complete discussion of these risks and the mitigating controls in place are documented in CM-7(2) Decision Log.  This decision log was reviewed as part of the 2017 FedRAMP audit and documented as an operational requirement in the 2017 FedRAMP SAR.  Office 365 MT has implemented blacklist detections. |

#### CM-7 (5) Control Enhancement (M)

The organization:

1. Identifies [Assignment: organization-defined software programs authorized to execute on the information system];
2. Employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the information system; and
3. Reviews and updates the list of authorized software programs [FedRAMP Assignment: at least annually or when there is a change].

| CM-7 (5) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager, Service Engineer Operations | |
| Parameter CM-07(5)(a):  software programs authorized to execute on the information system as defined in baselines and configuration scripts | |
| Parameter CM-07(5)(c):  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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| CM-7 (5) - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT identifies software authorized to execute within Office 365 MT via baseline configurations 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 Office 365 MT. All software goes through an approval process before being installed using the standard deployment process. |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT 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 Advisory Board (CAB). |
| Part c | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT service teams review and update baselines and configuration scripts at least annually. |

### CM-8 Information System Component Inventory (L) (M) (H)

The organization:

1. Develops and documents an inventory of information system components that:

Accurately reflects the current information system;

Includes all components within the authorization boundary of the information system;

Is at the level of granularity deemed necessary for tracking and reporting; and

Includes [Assignment: organization-defined information deemed necessary to achieve effective information system component accountability]; and

1. Reviews and updates the information system component inventory [FedRAMP Assignment: at least monthly].

CM-8 Additional FedRAMP Requirements and Guidance:

Requirement: Must be provided at least monthly or when there is a change.

| CM-8 | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager, Service Engineer Operations | |
| Parameter CM-08(a)(4):  • Server Name  • Data Center Name  • Asset Tag  • Location Name  • Asset Model Name  • Primary Property Name  • Manufacturer Name  • IP  • OS  • Role | |
| Parameter CM-08(b):  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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| CM-8 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  **Parts 1,2,3,4:**  Service teams within Office 365 are responsible for developing and documenting an inventory of components that accurately reflects their current information system, and includes all components within the authorization boundary.  Service teams provide their inventory to Office 365 Trust on a monthly basis. Office 365 Trust maintains tools which act as a central repository for aggregating inventories across all service teams.  Each inventory is at the level of granularity required by Office 365 Trust, and includes the fields required for import into the Office 365 trust tool. |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Service teams review and update their inventory on a monthly basis, and provide that inventory to Office 365 Trust. |

#### CM-8 (1) Control Enhancement (M) (H)

The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.

| CM-08(1) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager, 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| CM-08(1) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Service teams are responsible for maintaining inventories as part of component installations, removals, and information system updates. The updates to inventory are reflected in the monthly list each service team delivers to Office 365 Trust. |

#### CM-8 (3) Control Enhancement (M) (H)

The organization:

1. Employs automated mechanisms [FedRAMP Assignment: Continuously, using automated mechanisms with a maximum five-minute delay in detection] to detect the presence of unauthorized hardware, software, and firmware components within the information system; and
2. Takes the following actions when unauthorized components are detected: [Selection (one or more): disables network access by such components; isolates the components; notifies [Assignment: organization-defined personnel or roles]].

| CM-8 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Trust Program Manager | |
| Parameter CM-08(3)(a):  continuously, using automated mechanisms with a maximum five-minute delay in detection | |
| Parameter CM-08(3)(b):  disables network access by such components and notifies 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| CM-8 (3) - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  As documented in Decision Log “Monitoring and alerting of attached unauthorized devices in the Data Centers (AC-19)”, Azure has concluded that their physical and screening controls prevent a malicious individual from gaining physical access to the Office 365 hardware and connecting unapproved devices. |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  See CM-08(3)(a) |

#### CM-8 (5) Control Enhancement (M) (H)

The organization verifies that all components within the authorization boundary of the information system are not duplicated in other information system inventories.

| CM-08(5) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager, 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| CM-08(5) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Azure assigns every physical asset to a single property group. Each property group belongs to a single information system. This ensures that all components are assigned to one and only one information system. Office 365 MT inventory information includes the relevant property group for each physical asset. The continuous monitoring process ensures that duplication of components is captured and remediated. |

### CM-9 Configuration Management Plan (M) (H)

The organization develops, documents, and implements a configuration management plan for the information system that:

1. Addresses roles, responsibilities, and configuration management processes and procedures;
2. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;
3. Defines the configuration items for the information system and places the configuration items under configuration management; and
4. Protects the configuration management plan for unauthorized disclosure and modification.

| CM-9 | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Trust Program Manager, Program Manager | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| CM-9 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT has a system-wide configuration management plan titled Office 365 Configuration Management Plan, which addresses high-level roles and responsibilities and configuration management processes and procedures. Each service team complies with this configuration management plan. The plan is reviewed at least annually and is maintained by Office 365 Trust. |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT has a system-wide configuration management plan titled Office 365 Configuration Management Plan, which establishes processes for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items. Each service team complies with this configuration management plan. The plan is reviewed at least annually and is maintained by Office 365 Trust. |
| Part c | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT has a system-wide configuration management plan titled Office 365 Configuration Management Plan, which defines the configuration items for the information system and places the configuration items under configuration management. Each service team complies with this configuration management plan. The plan is reviewed at least annually and is maintained by Office 365 Trust. |
| Part d | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT has a system-wide configuration management plan titled Office 365 Configuration Management Plan. Each service team complies with this configuration management plan. The plan is reviewed at least annually, is maintained by Office 365 Trust, and is stored on the Office 365 Trust SharePoint, which has functionality to protect against unauthorized disclosure and modification. |

### CM-10 Software Usage Restrictions (L) (M) (H)

The organization:

1. Uses software and associated documentation in accordance with contract agreements and copyright laws;
2. Tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution; and
3. Controls and documents 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 Role: Office 365 Trust Program Manager, Program Manager | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| CM-10 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Microsoft Online Services Acceptable Use Policy outlines the Online Services specific acceptable usage standards of the Infrastructure & Services technology assets, and states:  “Any actions that violate the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of “pirated" or other software products that are not appropriately licensed for use by Microsoft are prohibited.” |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Information Security Policy outlines the software usage restrictions for Office 365 MT, and require all Office 365 MT applications, including those developed or hosted by and/or purchased from third parties, to undergo a comprehensive security review before entry into Microsoft Online environments. In addition, no software is to be deployed or utilized in the Service’s production environments without formal approval as required by Office 365 MT change management processes.  In-house software used within the Office 365 MT boundary is developed by Microsoft and, therefore, not subject to contractual requirements, copyright restrictions, and licenses monitoring for compliance with third-party relationships. In regard to third-party relationships, Microsoft complies with all software usage requirements as defined by the contractual agreement with the vendor.  Software is tracked through version history and documentation inside of source control tools. Documentation is tracked through SharePoint version control. |
| Part c | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT does not allow peer-to-peer file sharing. If the need arises to install a peer-to-peer file sharing application manager, CELA and Microsoft Information Security approval is required. |

#### CM-10 (1) Control Enhancement (M) (H)

The organization establishes the following restrictions on the use of open source software: [Assignment: organization-defined restrictions].

| CM-10(1) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Trust Program Manager, Program Manager | |
| Parameter CM-10(1):  All software (including tools and utilities) installed within the information system must be approved by the appropriate stakeholders prior to being released into production. Prior to deployment in the information system, 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. | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| CM-10(1) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The following restrictions are in place regarding the installation of software, including open source software, within the Office 365 MT environment:  • All software (including tools and utilities) installed within Office 365 MT must be approved by the appropriate stakeholders prior to being released into production.  • Prior to deployment in Office 365 MT, 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. |

### CM-11 User-Installed Software (M) (H)

The organization:

1. Establishes [Assignment: organization-defined policies] governing the installation of software by users;
2. Enforces software installation policies through [Assignment: organization-defined methods]; and
3. Monitors policy compliance [FedRAMP Assignment: Continuously (via CM-7 (5))].

| CM-11 | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Trust Program Manager, Program Manager | |
| Parameter CM-11(a):  defined policies | |
| Parameter CM-11(b):  a combination of RBAC and a formalized change management process | |
| Parameter CM-11(c):  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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| CM-11 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Information Security Policy and associated standards (provided) outlines the Microsoft user-installed software restrictions for Office 365 MT. In accordance with the policy, all software installed in the Microsoft Online Services environment, prior to being released into production, must go through the Microsoft change management process and be approved by the appropriate stakeholders.  As established by the Office 365 Information Security Policy, the following guidelines are in place regarding the installation of software, including open source software, within the Office 365 MT environment:  • All software (including tools and utilities) installed within Office 365 MT must be approved by the appropriate stakeholders prior to being released into production.  • Prior to deployment in Office 365 MT, 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). |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT enforces software installation policies through configuration control processes. Office 365 MT service administrators only install software approved through approved change management processes, as described in the Office 365 Configuration Management Plan. |
| Part c | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT monitors compliance continuously for the baseline. |

* 1. Contingency Planning (CP)

### CP-1 Contingency Planning Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:

A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

Procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls; and

1. Reviews and updates the current:
   1. Contingency planning policy [FedRAMP Assignment: at least every three (3) years].; and
   2. Contingency planning procedures [FedRAMP Assignment: at least annually].

| CP-1 | Control Summary Information |
| --- | --- |
| Responsible Role: BCM, Program Manager | |
| Parameter CP-01(a)(1):  Service Engineer Operations, Program Manager, Developer, Tester, Office 365 Trust Program Manager, Office 365 Security Manager, BCM | |
| Parameter CP-01(a)(2):  Service Engineer Operations, Program Manager, Developer, Tester, Office 365 Trust Program Manager, Office 365 Security Manager, BCM | |
| Parameter CP-01(b)(1):  annually | |
| Parameter CP-01(b)(2):  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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| CP-1 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Part 1:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Information Security Policy provides the overarching security guidance for Office 365 MT. This document addresses the purpose, scope, roles, responsibilities, compliance requirements, and required coordination among the various Microsoft organizations providing some level of support for the security of Office 365 MT. Policies distributed to personnel responsible for implementing contingency planning policies and procedures via SharePoint.  **Part 2:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Information Security Policy contains policies that must be met in the delivery and operation of Office 365 MT. Standards and procedures to facilitate execution of these policies are documented in the Active Framework Controls, Office 365 Standard Operating Procedures (SOPs), and service team-specific SOPs. These standards and procedures act as adjuncts to the security policy and provide implementation level requirements and details to carry out specific operational tasks. A detailed mapping of Office 365 standards and procedures to each control is available for review. Office 365 SOPs are distributed via SharePoint. |
| Part b | **Part 1:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Information Security Policy is reviewed and updated annually by the Office 365 Trust team.  **Part 2:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Standard Operating Procedures (SOPs) are reviewed and updated annually by the service teams and by Office 365 Trust. |

### CP-2 Contingency Plan (L) (M) (H)

The organization:

1. Develops a contingency plan for the information system that:
   1. Identifies essential missions 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 missions and business functions despite an information system disruption, compromise, or failure;
   5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and
   6. Is reviewed and approved by [Assignment: organization-defined personnel or roles];
2. Distributes copies of the contingency plan to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements];
3. Coordinates contingency planning activities with incident handling activities;
4. Reviews the contingency plan for the information system [FedRAMP Assignment: at least annually];
5. Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;
6. Communicates contingency plan changes to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]; and
7. Protects the contingency plan from unauthorized disclosure and modification.

CP-2 Additional FedRAMP Requirements and Guidance:

Requirement: For JAB authorizations, the contingency lists include designated FedRAMP personnel.

| CP-2 | Control Summary Information |
| --- | --- |
| Responsible Role: BCM, Program Manager | |
| Parameter CP-02(a)(6):  Office 365 Business Continuity Management (BCM) team | |
| Parameter CP-02(b):  BCM | |
| Parameter CP-02(d):  annually | |
| Parameter CP-02(f):  BCM | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| CP-2 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Part 1:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Each service team coordinates with the Business Continuity Management (BCM) team to develop and document a contingency plan that:  • Identifies essential missions and business functions and associated contingency requirements;  • Provides recovery objectives, restoration priorities, and metrics;  • Addresses contingency roles, responsibilities, and assigned individuals with contact information;  • Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;  • Addresses the eventual full information system restoration without deterioration of the security measures originally planned and implemented; and  • Is reviewed and approved by designated officials within the organization (documented)  Each service team’s plan is titled “[service team] Business Continuity Plan".  **Part 2:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  See CP-02(a)(1).  **Part 3:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  See CP-02(a)(1).  **Part 4:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  See CP-02(a)(1).  **Part 5:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  See CP-02(a)(1).  **Part 6:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  See CP-02(a)(1). |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The contingency plans are stored on a SharePoint site that is accessible to all service teams. Key personnel are identified by name and role within each plan. These key personnel are required to review the plan annually and the Business Continuity Management (BCM) team maintains a record of the review. |
| Part c | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Business Continuity Management (BCM) team coordinates with the Office 365 Security Incident & Response (SIR) team when determining plan requirements. Each plan includes instructions for coordinating plan execution with the incident handling process. |
| Part d | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 MT service team-specific Business Continuity Plans (BCP) are reviewed at least on an annual basis by the Office 365 Business Continuity Management (BCM) team and service-team specific business continuity teams (documented in service team BCPs). Business Continuity Plans will be updated with FedRAMP customer personnel as required by FedRAMP customers. |
| Part e | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 MT service team-specific business continuity plans are reviewed on an annual basis, as well as in response to changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing. Reviews are conducted by the Office 365 Business Continuity Management (BCM) team and service-team specific business continuity teams (documented in service team BCPs named “[service team] Business Continuity Plan”). |
| Part f | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  When changes are made to the plan, acceptance and approval are required by key personnel identified within the plan. The plan is then posted and stored in SharePoint. Business Continuity Plan changes will be provided for acceptance and approval to FedRAMP customer personnel as required by FedRAMP customers. |
| Part g | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT protects the contingency plan from unauthorized disclosure and modification by using access controls within SharePoint. Training and NDAs protect against the disclosure of information by support personnel. |

#### CP-2 (1) Control Enhancement (M) (H)

The organization coordinates contingency plan development with organizational elements responsible for related plans.

| CP-02(1) | Control Summary Information |
| --- | --- |
| Responsible Role: BCM, Program Manager | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| CP-02(1) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT coordinates contingency plan development with organizational elements responsible for related plans. The Business Continuity Plan (BCP) documents have been developed separately for each Office 365 MT service team. The Business Continuity Plans address the dependencies with other Office 365 MT service teams as well as any dependencies outside of Office 365 MT such as Azure. Office 365 Business Continuity Management (BCM) is responsible for coordinating between service teams and with external dependencies. |

#### CP-2 (2) Control Enhancement (M) (H)

The organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.

| CP-02(2) | Control Summary Information |
| --- | --- |
| Responsible Role: BCM, Program Manager | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| CP-02(2) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  All service teams include capacity planning as a key feature of their datacenter models and data replication plans to ensure that there is necessary capacity for information processing, telecommunications, and environmental support. |

#### CP-2 (3) Control Enhancement (M) (H)

The organization plans for the resumption of essential missions and business functions within [Assignment: organization-defined time period] of contingency plan activation.

| CP-02(3) | Control Summary Information |
| --- | --- |
| Responsible Role: BCM, Program Manager | |
| Parameter CP-02(3):  Recovery Time Objectives documented in service team BIAs | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| CP-02(3) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  All Office 365 MT service teams establish recovery time objectives (RTO) for essential Office 365 MT missions and business functions, and document those objectives in a Business Impact Analysis (BIA) as part of the Business Continuity Management (BCM) process. |

#### CP-2 (8) Control Enhancement (M) (H)

The organization identifies critical information system assets supporting essential missions and business functions.

| CP-02(8) | Control Summary Information |
| --- | --- |
| Responsible Role: BCM, Program Manager | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| CP-02(8) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  All Office 365 MT service teams identify critical information system assets for Office 365 MT services and document those assets in a Dependency Analysis as part of the Business Continuity Management (BCM) process. |

### CP-3 Contingency Training (L) (M) (H)

The organization provides contingency training to information system users consistent with assigned roles and responsibilities:

1. Within [FedRAMP Assignment: ten (10) days] of assuming a contingency role or responsibility;
2. When required by information system changes; and
3. [FedRAMP Assignment: at least annually] thereafter.

| CP-3 | Control Summary Information |
| --- | --- |
| Responsible Role: BCM, Program Manager | |
| Parameter CP-03(a):  10 days | |
| Parameter CP-03(c):  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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| CP-3 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT trains personnel in their contingency roles and responsibilities through their Office 365 Business Continuity Management (BCM) Training & Awareness program within 10 days of assuming a contingency role or responsibility. For all new service team personnel with contingency responsibilities, this training is incorporated into onboarding training. |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Contingency training will also be conducted as needed when required by information system changes. |
| Part c | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Contingency refresher training is provided annually. |

### CP-4 Contingency Plan Testing (H)

The organization:

1. Tests the contingency plan for the information system [FedRAMP Assignment: at least annually] using [FedRAMP Assignment: functional exercises] to determine the effectiveness of the plan and the organizational readiness to execute the plan;

CP-4(a) Additional FedRAMP Requirements and Guidance:

Requirement: The service provider develops test plans in accordance with NIST Special Publication 800-34 (as amended) and provides plans to FedRAMP prior to initiating testing. Test plans are approved and accepted by the JAB/AO prior to initiating testing.

1. Reviews the contingency plan test results; and
2. Initiates corrective actions, if needed.

| CP-4 | Control Summary Information |
| --- | --- |
| Responsible Role: BCM, Service Engineer Operations | |
| Parameter CP-04(a):  1. at least annually; 2. functional exercises | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| CP-4 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Each service team tests the contingency plan at least annually to determine the plan's effectiveness and the service team's readiness to execute the plan. Office 365 Business Continuity Management (BCM) coordinates an annual functional exercise with each service team and documents the results. This functional exercise is used to evaluate the Business Continuity Plan's effectiveness and Office 365 MT's ability to execute the plan. Any issues identified during the functional exercise are tracked to remediation by Office 365 Business Continuity Management (BCM) and a POA&M is opened if the issue meets the criteria requiring a POA&M. The plan is updated to reflect remediation activities, and after the plan is updated, the plan is distributed. |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Each service team, in coordination with Office 365 Business Continuity Management, reviews the contingency plan test/exercise results. After the failover exercise is completed for contingency planning, any findings are documented during the post-mortem. |
| Part c | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Each service team, in coordination with Office 365 Business Continuity Management, reviews the contingency plan test/exercise results and initiates corrective actions. The contingency plan document is updated to include the lessons learned and any necessary procedural changes/enhancements to the plan. |

#### CP-4 (1) Control Enhancement (M) (H)

The organization coordinates contingency plan testing and/or exercises with organizational elements responsible for related plans.

| CP-04(1) | Control Summary Information |
| --- | --- |
| Responsible Role: BCM, Program Manager | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| CP-04(1) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 Business Continuity Management (BCM) is responsible for conducting functional exercises with each service team. Related plans are identified in each service team’s business continuity plan. Office 365 BCM coordinates organizational elements responsible for these related plans as required to effectively test the plans' effectiveness and reliability. |

### CP-6 Alternate Storage Site (M) (H)

The organization:

1. Establishes an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information; and
2. Ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site.

| CP-6 | Control Summary Information |
| --- | --- |
| Responsible Role: Azure, Program Manager | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| CP-6 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT establishes alternate storage sites including necessary agreements to permit the storage and recovery of backup information. Active alternate sites are in place for each of the service teams. All alternate sites are active sites leveraging near real-time data replication. Each alternate site is redundant and managed by Azure. The recovery agreements with Azure are in accordance with the recovery time objectives established within the service teams’ Business Impact Analysis. |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT alternate storage sites are managed by Azure, which is an accredited federal system under FedRAMP. All storage sites have logical and physical security safeguards equivalent to that of the primary site. |

#### CP-6 (1) Control Enhancement (M) (H)

The organization identifies an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats.

| CP-06(1) | Control Summary Information |
| --- | --- |
| Responsible Role: Azure, Program Manager | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| CP-06(1) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Each Office 365 MT service team has identified an alternate storage site that is separated from the primary storage site so as not to be susceptible to the same hazards. Office 365 MT services operate in Active/Active configurations utilizing geographically distributed Azure datacenters. The alternate storage site(s) for each service are the same as the alternate processing site(s) for that service. The data center pairs are carefully chosen to provide geographically diverse data centers. |

#### CP-6 (3) Control Enhancement (M) (H)

The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

| CP-06(3) | Control Summary Information |
| --- | --- |
| Responsible Role: Azure, Program Manager | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| CP-06(3) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT has evaluated alternative storage sites to identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster. An area-wide disruption or disaster would not affect the Office 365 MT alternate storage sites since they are located in geographically separated regions for each system.  The identification and mitigation of potential accessibility problems to the alternate storage site is inherited from Azure, which has a FedRAMP P-ATO (F1209051525). |

### CP-7 Alternate Processing Site (M) (H)

The organization:

1. Establishes an alternate processing site including necessary agreements to permit the transfer and resumption of [Assignment: organization-defined information system operations] for essential missions/business functions within [FedRAMP Assignment: see additional FedRAMP requirements and guidance] when the primary processing capabilities are unavailable;

CP-7a Additional FedRAMP Requirements and Guidance:

Requirement: The service provider defines a time period consistent with the recovery time objectives and business impact analysis.

1. Ensures that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the organization-defined time period for transfer/resumption; and
2. Ensures that the alternate processing site provides information security safeguards equivalent to that of the primary site.

| CP-7 | Control Summary Information |
| --- | --- |
| Responsible Role: Azure, Program Manager | |
| Parameter CP-07(a):  1. all information system operations; 2. 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| CP-7 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Each Office 365 MT service team establishes an alternate processing site including necessary agreements to permit the resumption of all information system operations for essential missions and business functions within the recovery times documented in each service team’s Business Impact Analysis when the primary processing capabilities are unavailable.  Active alternate sites have been established for each of the service teams. All alternate sites are active sites as detailed in the specific Business Continuity Plan for each service team. Each alternate site is redundant and managed by Azure. The recovery agreements with Azure are in accordance with the recovery time objectives established within the Business Impact Analysis. |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT ensures that equipment and supplies required to resume operations are available at the alternate site or contracts are in place to support delivery to the site in time to support the time period for resumption defined in each service team’s Business Impact Analysis.  Because each site is operationally active, both the primary and the alternate site contain identical equipment to support ongoing production of the system due to a disruption at the other location. The recovery agreement with Azure is in accordance with the recovery time objectives established within the Business Impact Analysis. |
| Part c | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT alternate processing sites are managed by Azure, which is an accredited federal system under FedRAMP. Alternate storage sites have physical security safeguards equivalent to that of the primary site. All storage sites have logical safeguards equivalent to that of the primary storage site.  The establishment of physical and network security safeguards equivalent to that of the primary site is inherited from Azure, which has a FedRAMP P-ATO (F1209051525). |

#### CP-7 (1) Control Enhancement (M) (H)

The organization identifies an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats.

CP-7(1) Additional FedRAMP Requirements and Guidance

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-07(1) | Control Summary Information |
| --- | --- |
| Responsible Role: Azure, Program Manager | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| CP-07(1) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The alternate processing sites for each Office 365 MT service team are separated as to not be susceptible to the same hazards, as detailed in the Business Continuity Plan applicable to each system. Office 365 MT services operate in Active/Active configurations utilizing geographically distributed Azure datacenters. The data center pairs are carefully chosen to provide geographically diverse data centers. |

#### CP-7 (2) Control Enhancement (M) (H)

The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

| CP-07(2) | Control Summary Information |
| --- | --- |
| Responsible Role: Program Manager | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| CP-07(2) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  After evaluating the geographical distribution of the alternate sites, Office 365 MT personnel have determined that an area-wide disruption or disaster would not affect the respective Office 365 MT alternate processing sites since they are located in different regions of the United States for each system. |

#### CP-7 (3) Control Enhancement (M) (H)

The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives).

| CP-07(3) | Control Summary Information |
| --- | --- |
| Responsible Role: Program Manager | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| CP-07(3) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT service teams develop alternate processing site agreements that contain priority-of-service provisions in accordance with the organization’s availability requirements. Recovery time objectives (RTO) are established for Office 365 MT services and are detailed as part of the Business Continuity Management (BCM) process. These RTOs serve as the alternate processing site agreements which determine the priority-of-service provisions for each Office 365 MT service. |

### CP-8 Telecommunications Services (M) (H)

The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of [Assignment: organization-defined information system operations] for essential missions and business functions within [FedRAMP Assignment: See CP-8 additional FedRAMP requirements and guidance] when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

CP-8 Additional FedRAMP Requirements and Guidance:

Requirement: The service provider defines a time period consistent with the recovery time objectives and business impact analysis.

| CP-08 | Control Summary Information |
| --- | --- |
| Responsible Role: Azure | |
| Parameter CP-08:  1. all information system operations; 2. recovery time objectives identified in service team BIAs | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| CP-08 - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  This control is inherited from Azure, which has a FedRAMP P-ATO (F1209051525). |

#### CP-8 (1) Control Enhancement (M) (H)

The organization:

1. Develops primary and alternate telecommunications service agreements that contain priority- of-service provisions in accordance with organizational availability requirements (including recovery time objectives); and
2. Requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier.

| CP-8 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| CP-8 (1) - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  This control is inherited from Azure, which has a FedRAMP P-ATO (F1209051525). |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  This control is inherited from Azure, which has a FedRAMP P-ATO (F1209051525). |

#### CP-8 (2) Control Enhancement (M) (H)

The organization obtains alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.

| CP-08(2) | Control Summary Information |
| --- | --- |
| Responsible Role: 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| CP-08(2) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  This control is inherited from Azure, which has a FedRAMP P-ATO (F1209051525). |

### CP-9 Information System Backup (L) (M) (H)

The organization:

CP-9 Additional FedRAMP Requirements and Guidance:

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.

1. Conducts backups of user-level information contained in the information system [FedRAMP Assignment: daily incremental; weekly full]

CP-9 (a) Additional FedRAMP Requirements and Guidance:

Requirement: The service provider maintains at least three backup copies of user-level information (at least one of which is available online).

1. Conducts backups of system-level information contained in the information system [FedRAMP Assignment: daily incremental; weekly full];

CP-9 (b) Additional FedRAMP Requirements and Guidance:

Requirement: The service provider maintains at least three backup copies of system-level information (at least one of which is available online).

1. Conducts backups of information system documentation including security-related documentation [FedRAMP Assignment: daily incremental; weekly full]; and

CP-9 (c) Additional FedRAMP Requirements and Guidance:

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).

1. Protects the confidentiality, integrity, and availability of backup information at storage locations.

| CP-9 | Control Summary Information |
| --- | --- |
| Responsible Role: Azure, Service Engineer Operations | |
| Parameter CP-09(a):  daily incremental, weekly full | |
| Parameter CP-09(b):  daily incremental, weekly full | |
| Parameter CP-09(c):  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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| CP-9 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Bing:**  Physical backups are not used. Data is continuously replicated and paired with one or more active sites to support disaster recovery.  **DNS, SUE, SWE, WAC:**  This is N/A; these service teams do not store user-level information.  **EXO:**  All EXO data is continuously replicated between instances and across multiple sites. In addition, messages are recoverable for 7 days after deletion.  **IP:**  Email is shadowed between data centers; if processing in one data center fails, the other data center automatically picks up the processing.  **Delve, MSTeams, OLM, OSI:**  Physical backups are not used. Data is continuously replicated using either Azure's built in data replication or complete redundant services.  **SFB:**  SFB deploys pairs of Front End pools across two geographically dispersed sites. Each site contains a Front-End pool which is paired with a corresponding Front End pool in the other site. Both sites are active, and the Lync Server Backup Service provides real-time data replication to keep the pools synchronized. The Backup Service is designed to support the disaster recovery solution. For capacity planning purposes, each pool is designed to handle the workloads of all users in both pools in the event of a disaster. In the event of the need to completely rebuild the system, a combination of system images and Customer Specific Settings files would be used.  See the following TechNet article for more information about deploying paired Front-End pools for disaster recovery in Lync Server 2013: https://technet.microsoft.com/en-us/library/jj204773.aspx  **SPO:**  The service team conducts weekly full backups and daily differential backups and backs up the transaction logs every five minutes. Backups are stored in Azure Storage. Backups are retained for at least 15 days, and backups are replicated to an alternate site.  The use of Azure Storage is inherited from Azure, which has a FedRAMP IaaS P-ATO (package ID F1209051525). |
| Part b | **Bing:**  Physical backups are not used. Data is continuously replicated and paired with one or more active sites to support disaster recovery.  **Delve, MSTeams, OLM, OSI:**  Physical backups are not used. Data is replicated using either Azure's built in data replication, or complete redundant services.  **DNS:**  Office 365 DNS has implemented a scheduled script that verifies media reliability and information integrity of its online backups weekly using System Center Data Protection Manager. The backups contain 30 days of full daily backups of the DNS databases. All other DNS service information can be restored using standard deployment processes.  **EXO, SPO:**  System-level backups are not performed. Standard images and scripts are used to recover lost servers, and replicated data is used to restore customer user-level data.  **IP:**  Servers are stateless; server recovery consists of redeployment from standard images and scripts. Databases (mail trace information, MX records, spam definitions, etc.) are replicated between data centers.  **MA:**  System-level information is backed up daily using geo-redundant Azure Storage.  **SFB:**  System-level backups are not performed. Daily incremental and weekly full backups are conducted for SQL server schemas, and AD information is backed up through replication across sites and data centers. SQL server schemas are stored for no less than 30 days and geo-replicated to alternate data centers for high availability.  **SUE:**  Operating system and specific build information is stored by Azure, and source code for the SUE application is stored in Source Depot.  **SWE:**  SWE employs SCRAM database backup using the Azure SQL backup tool to encrypt into blob storage daily.  **WAC:**  Servers are stateless; server recovery consists of redeployment from standard images and scripts per the configuration management process. |
| Part c | **DNS:**  System documentation is stored on SharePoint. Office 365 DNS specific code is maintained both in compiled form on utility servers within each datacenter and in uncompiled form in Source Depot. The compiled form is not explicitly backed up given it can be recompiled on demand and moved back into any given production environment using standard deployment processes. Both SharePoint and Source Depot use versioning and are replicated in near real time.  **Bing, Delve, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT maintains backups of information system documentation, including security-related documentation, through SharePoint and Source Depot replication. System documentation is stored on SharePoint, and Source Depot contains system and application images. Both SharePoint and Source Depot use versioning and are replicated in near real time. |
| Part d | **Bing:**  Physical backups are not used. Data is continuously replicated and paired with one or more active sites to support disaster recovery.  **Delve, OLM, OSI, SUE:**  Delve, OLM, OSI, and SUE inherit this control from Azure. Azure has a FedRAMP IaaS P-ATO (package ID F1209051525).  **DNS:**  In addition to the secure replication solution in place, Office 365 DNS uses System Center Data Protection Manger for physical backups. All data that is backed up is encrypted prior to writing to disk, which protects both the confidentiality and integrity of the backed-up data.  **EXO, IP, MSTeams, SPO, SWE, WAC:**  Physical backups are not used. Data is replicated through secure channels to protect the confidentiality, integrity, and availability of the information.  **SFB:**  Online backup data is stored within the accreditation boundary and protected via the same methods as production data. Data that is physically backed up is encrypted prior to writing to tape or disk, which protects both the confidentiality and integrity of the backed-up data. |

#### CP-9 (1) Control Enhancement (M)

The organization tests backup information [FedRAMP Assignment: at least annually] to verify media reliability and information integrity.

| CP-09(1) | Control Summary Information |
| --- | --- |
| Responsible Role: Service Engineer Operations | |
| Parameter CP-09(1):  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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| CP-09(1) - What is the solution and how is it implemented? |
| --- |
| **DNS:**  In addition to replication solutions, Office 365 DNS uses System Center Data Protection Manager. All data that is backed up is encrypted prior to writing to disk which protects both the confidentiality and integrity of the backed-up data. DNS has implemented a scheduled script that verifies media reliability and information integrity of its backups weekly.  **Bing, Delve, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  These service teams do not use any media backups. These service teams utilize Data Center replication solutions. Each service team's Business Continuity Plan indicates the procedures in place for the replication of Office 365 MT data. Service teams perform failovers monthly as a part of testing, patching or routine service. Continuous monitoring is used to alert on failures of service reliability and integrity, that may necessitate a failover. |

#### CP-9 (3) Control Enhancement (M) (H)

The organization stores backup copies of [Assignment: organization-defined critical information system software and other security-related information] in a separate facility or in a fire-rated container that is not collocated with the operational system.

| CP-09(3) | Control Summary Information |
| --- | --- |
| Responsible Role: Service Engineer Operations | |
| Parameter CP-09(3):  critical information system software and other security-related information as documented in "Defining critical information system software and other security-related information Decision Log (CP-9(3))" | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| CP-09(3) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT has defined critical information system software and other security-related information as documented in “Defining critical information system software and other security-related information decision log (CP-9(3))”. This critical functionality and data is replicated and stored across at least two data centers. |

### CP-10 Information System Recovery and Reconstitution (L) (M) (H)

The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.

| CP-10 | Control Summary Information |
| --- | --- |
| Responsible Role: Azure, 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| CP-10 - What is the solution and how is it implemented? |
| --- |
| **DNS:**  The DNS Business Continuity Plan provides for the recovery and reconstitution of DNS to a known state after a disruption, compromise, or failure. Office 365 DNS maintains online the geo-diverse set of DNS databases using System Center Data Protection Manager (DPM). The backups contain 30 days of full daily backups of the DNS databases. No other information is stateful and the DNS service can be restored using standard deployment processes.  This enables Office 365 DNS to restore operations from a total catastrophic failure to a known working state no older than 24 hours from the last backup execution. The DPM backups execute twice daily.  **Bing, Delve, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Business Continuity Plan documents (named "[service team] Business Continuity Plan") developed separately for the Office 365 MT systems outlined above provide for the recovery and reconstitution of each system to a known state after a disruption, compromise, or failure. The Business Continuity Plan documentation states, on a detailed step-by-step basis, the tasks to recover each Office 365 MT system outlined above.  If all primary and secondary Data Centers for an Office 365 MT system experience failure or if Microsoft were to resume processing at a disrupted site, Microsoft will use the following to recover Office 365 MT systems in other Azure managed Data Centers to the last known state:  • Defined images and current O/S and application baselines  • Defined security processes, such as access control, change management, and encryption mechanisms  • Defined vulnerability and patch process to properly maintain new systems |

#### CP-10 (2) Control Enhancement (M) (H)

The information system implements transaction recovery for systems that are transaction-based.

| CP-10(2) | Control Summary Information |
| --- | --- |
| Responsible Role: 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869) | |

| CP-10(2) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT does not use transaction-based systems. |

* 1. Identification and Authentication (IA)

### IA-1 Identification and Authentication Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls; and
2. Reviews and updates the current:
   1. Identification and authentication policy [FedRAMP Assignment: at least every three (3) years]; and
   2. Identification and authentication procedures [FedRAMP Assignment: at least annually].

| IA-1 | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Trust Program Manager | |
| Parameter IA-01(a)(1):  Service Engineer Operations, Program Manager, Developer, Tester, Office 365 Trust Program Manager, Office 365 Security Manager, BCM | |
| Parameter IA-01(a)(2):  Service Engineer Operations, Program Manager, Developer, Tester, Office 365 Trust Program Manager, Office 365 Security Manager, BCM | |
| Parameter IA-01(b)(1):  annually | |
| Parameter IA-01(b)(2):  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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| IA-1 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Part 1:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Information Security Policy provides the overarching security guidance for Office 365 MT. This document addresses the purpose, scope, roles, responsibilities, compliance requirements, and required coordination among the various Microsoft organizations providing some level of support for the security of Office 365 MT. The Office 365 Information Security Policy is distributed to personnel responsible for implementing identification and authentication policies and procedures via SharePoint.  **Part 2:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Standards and procedures to facilitate execution of these policies are documented in the Active Framework Controls, Office 365 Standard Operating Procedures (SOPs), and service team-specific SOPs. These standards and procedures act as adjuncts to the Office 365 Information Security Policy and provide implementation level requirements and details to carry out specific operational tasks. A detailed mapping of Office 365 standards and procedures to each control is available for review. Office 365 SOPs are distributed via SharePoint. |
| Part b | **Part 1:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Information Security Policy is reviewed and updated annually.  **Part 2:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Standard Operating Procedures (SOP) are reviewed and updated annually. |

### IA-2 User Identification and Authentication (L) (M) (H)

The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

| IA-02 | Control Summary Information |
| --- | --- |
| Responsible Role: Customer Administrator, Office 365 Security Manager, 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| IA-02 - What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility:**  All customers using ADFS authentication, including government customers and non-government customers, are responsible for uniquely identifying and authenticating their organizational users via their Active Directory infrastructure. When a user of an organization employing ADFS attempts to access Office 365 MT, the user is redirected to a login page hosted on the customer’s ADFS server. The user provides their credentials to their ADFS server, which attempts to authenticate the credentials using the customer’s existing Active Directory infrastructure. If the credentials are authenticated, the customer’s ADFS server issues a SAML ticket containing information about the user’s identity and group membership. The customer ADFS server signs this ticket using one half of an asymmetric key pair and the user sends the ticket to Azure Active Directory (AAD) via encrypted TLS. AAD validates the signature using the other half of the asymmetric key pair and grants access based on the ticket. Customers are responsible for enforcing organizationally appropriate identification and authentication requirements at their ADFS server, including the use of unique identifiers.  For more information on Active Directory object naming, see TechNet article 977992: http://Technet.microsoft.com/en-us/library/cc977992.aspx  Non-government customers not using ADFS to manage identification and authentication inherit these controls from AAD. When users enter their username at the Office 365 MT hosted login screen, AAD matches the user’s domain to the appropriate Active Directory Organizational Unit and attempts to establish a secure session with the user’s client. Once the session is established, AAD validates the user’s authenticators and issues the user a SAML ticket containing information about the user’s unique identity and group membership. Customer administrators use the SUE administration portal to set identification and authentication requirements for their organization. AAD enforces unique identifiers for these customers.  For more information on Active Directory object naming, see TechNet article 977992: http://Technet.microsoft.com/en-us/library/cc977992.aspx  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The service teams maintain Active Directory and Azure Active Directory (AAD) deployments for identifying and authenticating Microsoft users in the environment. Office 365 MT support personnel accessing Office 365 MT are uniquely identified by their Active Directory or AAD username and authenticate using eAuth Level 4 and FIPS 140-2 compliant Gemalto smartcards or approved eAuth Level 4 and FIPS 140-2 compliant TPM modules. Active Directory strictly enforces unique identifiers. OLM also uses YubiKeys with RSA certificates.  For more information on Active Directory object naming, see TechNet article 977992: http://Technet.microsoft.com/en-us/library/cc977992.aspx |

#### IA-2 (1) Control Enhancement (L) (M) (H)

The information system implements multifactor authentication for network access to privileged accounts.

| IA-02(1) | Control Summary Information |
| --- | --- |
| Responsible Role: Customer Administrator, Office 365 Security Manager, 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| IA-02(1) - What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility:**  Government customers are required to use HSPD-12 compliant multifactor authentication for all access to Office 365 MT. Office 365 MT requires customers to implement ADFS to leverage organizational multifactor authentication solutions, including HSPD-12, already deployed to meet their internal identification and authentication requirements. Customers configure their ADFS server to enforce identification and authentication requirements; ADFS uses the same multifactor authentication as the customer’s internal Active Directory/Domain infrastructure.  For more information about configuring customer ADFS server(s) to enforce multifactor authentication, see section 6.2 of the following document: http://download.microsoft.com/download/0/7/1/07156662-5B63-404A-8E36-5446FA06A0B0/Office365-Single%20Sign-On-with-AD-FS2.0-v1.0a.docx  Non-government customers may not be required to implement multifactor authentication. Non-government customers may implement multifactor authentication following the same procedures outlined for government customers (above) or they may elect to allow access using single factor authentication. Customers are responsible for determining the access requirements appropriate for the risk tolerances of their system and information.  Guest access to SFB meetings, if enabled, is via single factor authentication. Government and non-government customers are responsible for determining if the use of guest access to SFB sessions should be allowed for their organization. This setting can be configured by government and non-government customers. For more information, see the following TechNet article: http://technet.microsoft.com/en-US/library/gg398648.aspx  Guest access to SharePoint Online, if enabled, is via single factor authentication. Government and non-government customers are responsible for determining if the use of guest access to SharePoint Online should be allowed for their organization. This setting can be configured by government and non-government customers. For more information, see the following Office 365 help article: http://office.microsoft.com/en-us/office365-sharepoint-online-small-business-help/manage-sharing-with-external-users-HA102849862.aspx  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT implements multifactor authentication for network access by Office 365 MT personnel through the use of eAuth Level 4 and FIPS 140-2 compliant Gemalto smartcards or approved eAuth Level 4 and FIPS 140-2 compliant TPM modules. |

#### IA-2 (2) Control Enhancement (M) (H)

The information system implements multifactor authentication for network access to non-privileged accounts.

| IA-02(2) | Control Summary Information |
| --- | --- |
| Responsible Role: Customer Administrator, 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| IA-02(2) - What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility:**  Government customers are required to use HSPD-12 compliant multifactor authentication for all access to Office 365 MT. Office 365 MT requires customers to implement ADFS to leverage organizational multifactor authentication solutions, including HSPD-12, already deployed to meet their internal identification and authentication requirements. Customers configure their ADFS server to enforce identification and authentication requirements; ADFS uses the same multifactor authentication as the customer’s internal Active Directory/Domain infrastructure.  For more information about configuring customer ADFS server(s) to enforce multifactor authentication, see section 6.2 of the following document: http://download.microsoft.com/download/0/7/1/07156662-5B63-404A-8E36-5446FA06A0B0/Office365-Single%20Sign-On-with-AD-FS2.0-v1.0a.docx  Non-government customers may not be required to implement multifactor authentication. Non-government customers may implement multifactor authentication following the same procedures outlined for government customers (above) or they may elect to allow access using single factor authentication. Customers are responsible for determining the access requirements appropriate for the risk tolerances of their system and information.  Guest access to SFB meetings, if enabled, is via single factor authentication. Government and non-government customers are responsible for determining if the use of guest access to SFB sessions should be allowed for their organization. This setting can be configured by government and non-government customers. For more information, see the following TechNet article: http://technet.microsoft.com/en-US/library/gg398648.aspx  Guest access to SharePoint Online, if enabled, is via single factor authentication. Government and non-government customers are responsible for determining if the use of guest access to SharePoint Online should be allowed for their organization. This setting can be configured by government and non-government customers. For more information, see the following Office 365 help article: http://office.microsoft.com/en-us/office365-sharepoint-online-small-business-help/manage-sharing-with-external-users-HA102849862.aspx  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  All Office 365 MT accounts used by Office 365 MT personnel are considered privileged. Multifactor authentication is implemented for all Office 365 MT accounts. |

#### IA-2 (3) Control Enhancement (M) (H)

The information system implements multifactor authentication for local access to privileged accounts.

| IA-02(3) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| IA-02(3) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  As general practice, there is no local access to the Office 365 MT environment. Office 365 MT personnel do not have physical access to Office 365 MT servers, and Azure personnel do not have logical access to Office 365 MT servers. Events which might require local access in other environments usually result in replacement of hardware in the Office 365 MT environment. If local access is needed, it is only granted by following the incident response process. |

#### IA-2 (5) Control Enhancement (M) (H)

The organization requires individuals to be authenticated with an individual authenticator when a group authenticator is employed.

| IA-02(5) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| IA-02(5) - What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility:**  All customers using ADFS authentication, including government customers and non-government customers, are responsible for uniquely identifying individuals using group authenticators.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Group authenticators are not used by Office 365 MT. |

#### IA-2 (8) Control Enhancement (M) (H)

The information system implements replay-resistant authentication mechanisms for network access to privileged accounts.

| IA-02(8) | Control Summary Information |
| --- | --- |
| Responsible Role: Azure, Office 365 Security Manager, 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| IA-02(8) - What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility:**  Government customers are required to use HSPD-12 compliant multifactor authentication for all access to Office 365 MT. Office 365 MT requires customers to implement ADFS to leverage organizational, multifactor authentication solutions, including HSPD-12, already deployed to meet their internal identification and authentication requirements. Customers configure their ADFS server to enforce identification and authentication requirements; ADFS uses the same multifactor authentication, including replay resistance, as the customer’s internal Active Directory/Domain infrastructure.  For more information about configuring customer ADFS server(s) to enforce multifactor authentication, see section 6.2 of the following document: http://download.microsoft.com/download/0/7/1/07156662-5B63-404A-8E36-5446FA06A0B0/Office365-Single%20Sign-On-with-AD-FS2.0-v1.0a.docx  Non-government customers not using ADFS authenticate directly to Azure Active Directory (AAD). AAD is responsible for implementing replay-resistant authentication mechanisms for these customers.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT uses multifactor authentication for network access to privileged accounts by Office 365 MT personnel through the use of eAuth Level 4 and FIPS 140-2 compliant Gemalto smartcards or approved eAuth Level 4 and FIPS 140-2 compliant TPM modules. OLM also uses YubiKeys with RSA certificates.  Access to the Office 365 MT production environment using the smartcard/TPM module solution is protected from replay attacks by the built-in Kerberos 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. During authentication, the timestamp is checked and if the timestamp is earlier than or the same as a previous authenticator, the authentication request is denied.  For more information on Active Directory and Kerberos, see TechNet article 742516: http://technet.microsoft.com/en-us/library/bb742516.aspx |

#### IA-2 (11) Control Enhancement (M) (H)

The information system implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets [FedRAMP Assignment: FIPS 140-2, NIAP\* Certification, or NSA approval].

\*National Information Assurance Partnership (NIAP)

Additional FedRAMP Requirements and Guidance:

Guidance: PIV = separate device. Please refer to NIST SP 800-157 Guidelines for Derived Personal Identity Verification (PIV) Credentials. FIPS 140-2 means validated by the Cryptographic Module Validation Program (CMVP).

| IA-02(11) | Control Summary Information |
| --- | --- |
| Responsible Role: Azure, Office 365 Security Manager, Service Engineer Operations | |
| Parameter IA-02(11):  approved PKI Class 3 certificates | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| IA-02(11) - What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility:**  Government customers are required to use HSPD-12 compliant multifactor authentication for all access to Office 365 MT. Office 365 MT requires customers to implement ADFS to leverage organizational multifactor authentication solutions, including HSPD-12, already deployed to meet their internal identification and authentication requirements. Customers configure their ADFS server to enforce identification and authentication requirements; ADFS uses the same multifactor authentication as the customer’s internal Active Directory/Domain infrastructure.  For more information about configuring customer ADFS server(s) to enforce multifactor authentication, see section 6.2 of the following document: http://download.microsoft.com/download/0/7/1/07156662-5B63-404A-8E36-5446FA06A0B0/Office365-Single%20Sign-On-with-AD-FS2.0-v1.0a.docx  Non-government customers may not be required to implement multifactor authentication. Non-government customers may implement multifactor authentication following the same procedures outlined for government customers (above) or they may elect to allow access using single factor authentication. Customers are responsible for determining the access requirements appropriate for the risk tolerances of their system and information.  Guest access to SFB meetings, if enabled, is via single factor authentication. Government and non-government customers are responsible for determining if the use of guest access to SFB sessions should be allowed for their organization. This setting can be configured by government and non-government customers. For more information, see the following TechNet article: http://technet.microsoft.com/en-US/library/gg398648.aspx  Guest access to SharePoint Online, if enabled, is via single factor authentication. Government and non-government customers are responsible for determining if the use of guest access to SharePoint Online should be allowed for their organization. This setting can be configured by government and non-government customers. For more information, see the following article: http://office.microsoft.com/en-us/office365-sharepoint-online-small-business-help/manage-sharing-with-external-users-HA102849862.aspx  **Bing, Delve, DNS, EXO, IP, MSTeams, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT uses multifactor authentication for remote access by Office 365 MT personnel through the use of eAuth Level 4 and FIPS 140-2 compliant Gemalto smartcards or approved eAuth Level 4 and FIPS 140-2 compliant TPM modules. The decision log “TPM approval decision log” documents Office 365 MT’s assessment that TPM modules are sufficiently isolated to be considered separate from the system gaining access.  **OLM**:  Office 365 MT Outlook Mobile uses multifactor authentication for remote access by Office 365 MT personnel through the use of eAuth Level 4 and FIPS 140-2 compliant Gemalto smartcards or YubiKeys with RSA certificates. |

#### IA-2 (12) Control Enhancement (L) (M) (H)

The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials.

IA-2 (12) Additional FedRAMP Requirements and Guidance:

Guidance: Include Common Access Card (CAC), i.e., the DoD technical implementation of PIV/FIPS 201/HSPD-12.

| IA-02(12) | Control Summary Information |
| --- | --- |
| Responsible Role: Customer Administrator | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| IA-02(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.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT does not utilize Personal Identity Verification (PIV) credentials for service team administrators. PIV cards are not available to Office 365 MT service team personnel. As such this control is not applicable to Office 365 MT service team personnel. |

### IA-3 Device Identification and Authentication (M) (H)

The information system uniquely identifies and authenticates [Assignment: organization-defined specific and/or types of devices] before establishing a [Selection (one or more): local; remote; network] connection.

| IA-03 | Control Summary Information |
| --- | --- |
| Responsible Role: Service Engineer Operations | |
| Parameter IA-03:  1. all devices within the information system accreditation boundary; 2. 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| IA-03 - What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility:**  Government Customers are required to ensure their information systems uniquely identify and authenticate approved device types prior to establishing a connection with Office 365 MT.  Non-Government Customers may not be required to provide a list of approved devices prior to establishing a connection with Office 365 MT. Non-Government customers should implement industry best practices to determine connection requirements appropriate for the risk tolerances of their system and information.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT uses Active Directory to uniquely identify and authenticate all devices within the Office 365 MT boundary before establishing a network connection. All Office 365 MT physical servers are joined to an Active Directory domain when deployed. Active Directory Forest members are uniquely identified by Universally Unique Identifiers (UUIDs) with device authentication performed using Kerberos, which is a part of the Windows networking protocols.  When establishing a Microsoft Azure subscription, a subscription ID is created. The Fabric Controller (FC), which manages all VMs in Microsoft Azure, uses this subscription ID to tie VMs to particular subscriptions. For more information about the Fabric Controller see the Azure SSP.  For teams managed by PilotFish, an identity certificate is distributed to every machine on a PilotFish cluster. Each identity certificate contains a unique identifier (machine name), the environment, and machine function (server role). |

### IA-4 Identifier Management (L) (M)

The organization manages information system identifiers for users and devices by:

1. Receiving authorization from [Assignment: organization-defined personnel or roles] to assign an individual, group, role, or device identifier;
2. Selecting an identifier that identifies an individual, group, role, or device;
3. Assigning the identifier to the intended individual, group, role, or device;
4. Preventing reuse of identifiers for [FedRAMP Assignment: at least two (2) years]; and

Disabling the identifier after [FedRAMP Assignment: ninety days for user identifiers (see additional requirements and guidance)]

IA-4e Additional FedRAMP Requirements and Guidance:

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 http://iase.disa.mil/cloud\_security/Pages/index.aspx.

| IA-4 | Control Summary Information |
| --- | --- |
| Responsible Role: Customer Administrator, Azure, Office 365 Security Manager, Program Manager | |
| Parameter IA-04(a):  account managers identified in Microsoft account management tools | |
| Parameter IA-04(d):  all time | |
| Parameter IA-04(e):  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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| IA-4 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility:**  All customers, including government customers and non-government customers, are responsible for receiving authorization from designated organizational officials before assigning identifiers.  Customers using ADFS will assign identifiers in their own Active Directory infrastructure. Customers not using ADFS will assign identifiers in AAD via SUE.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  All Microsoft administrators must receive management authorization before being granted a Microsoft user identifier in any of the Office 365 MT domains. Authorization for administrator identifiers is managed through Microsoft account management tools. Device identifiers are authorized by service team administrators when adding new devices to the network, consistent with configuration management and inventory management procedures.  For teams using PilotFish, information system identifiers are managed by the PilotFish public key infrastructure. |
| Part b | **Customer Responsibility:**  All customers using ADFS authentication, including government customers and non-government customers, are responsible for selecting and assigning user identifiers via their Active Directory infrastructure.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  User identifiers are distributed to Office 365 MT administrators by their manager during the account creation process. Device identifiers are automatically assigned as part of the domain-joining process. Identifiers for groups and roles are assigned by Office 365 MT administrators. Active Directory enforces unique identifiers for users, groups, roles, and devices. For more information on Active Directory object naming, see TechNet article 977992: http://technet.microsoft.com/en-us/library/cc977992.aspx  For teams using PilotFish, information system identifiers are managed by the PilotFish public key infrastructure. Each PilotFish cluster has a designated Certificate Authority which distributes an identity certificate to each machine in the cluster. PilotFish identity certificates contain a unique identifier (machine name), the environment, and the machine function (server role). |
| Part c | **Customer Responsibility:**  All customers using ADFS authentication, including government customers and non-government customers, are responsible for selecting and assigning user identifiers via their Active Directory infrastructure.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  User identifiers are distributed to Office 365 MT administrators by their manager during the account creation process. Device identifiers are automatically assigned as part of the domain-joining process. Identifiers for groups and roles are assigned by Office 365 MT administrators. Active Directory enforces unique identifiers for users, groups, roles, and devices. For more information on Active Directory object naming, see TechNet article 977992: http://technet.microsoft.com/en-us/library/cc977992.aspx  For teams using PilotFish, information system identifiers are managed by the PilotFish public key infrastructure. Each PilotFish cluster has a designated Certificate Authority which distributes an identity certificate to each machine in the cluster. |
| Part d | **Customer Responsibility:**  All customers using ADFS authentication, including government customers and non-government customers, are responsible for preventing the reuse of user identifiers via their Active Directory infrastructure.  Customers not using ADFS are responsible for not reusing user identifiers.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Unique user, device, role, and group identifiers (UUIDs) are never reused. This is enforced by Active Directory and LDAP.  For teams using PilotFish, each machine on a PilotFish cluster is issued an identity certificate. PilotFish identity certificates are never reused. |
| Part e | **Customer Responsibility:**  All customers using ADFS authentication, including government customers and non-government customers, are responsible for disabling inactive user identifiers via their Active Directory infrastructure.  For customers not using ADFS, Azure Active Directory (AAD) does not automatically disable inactive user identifiers.  **DNS:**  DNS accounts are managed through OneIdentity; Azure is responsible for disabling identifiers after 90 days of inactivity.  **Bing, Delve, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Microsoft account management tools automatically disable Office 365 MT administrator accounts access to Terminal Services Gateways (TSGs) or SSH Gateways after at most 90 days of inactivity. Each service team disables service team domain accounts after at most 90 days of inactivity using a scheduled script that runs daily. |

#### IA-4 (4) Control Enhancement (M) (H)

The organization manages individual identifiers by uniquely identifying each individual as [FedRAMP Assignment: contractors; foreign nationals].

| IA-04(4) | Control Summary Information |
| --- | --- |
| Responsible Role: MSIT | |
| Parameter IA-04(4):  contractors or 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| IA-04(4) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Citizenship/contractor status of Microsoft employees is recorded in Microsoft account management tools which act as the authoritative systems for controlling/authorizing account permissions within Office 365 MT. Additionally, contractors and vendors are denoted by a prefix ("a-" or "v-", respectively) in the username.  Microsoft account management tools include citizenship information as part of the user record, but not in the identifier itself. |

### IA-5 Authenticator Management (L) (M)

The organization manages information system authenticators by:

1. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;
2. Establishing initial authenticator content for authenticators defined by the organization;
3. Ensuring that authenticators have sufficient strength of mechanism for their intended use;
4. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;
5. Changing default content of authenticators prior to information system installation;
6. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;
7. Changing/refreshing authenticators [FedRAMP Assignment: to include sixty (60) days for passwords].
8. Protecting authenticator content from unauthorized disclosure and modification;
9. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and
10. Changing authenticators for group/role accounts when membership to those accounts changes.

| IA-5 | Control Summary Information |
| --- | --- |
| Responsible Role: Customer Administrator, MSIT, Service Engineer Operations | |
| Parameter IA-05(g):  60 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| IA-5 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility:**  Office 365 MT customers are responsible for distributing authenticators in compliance with their organizational policies and requirements for their organizational users. Government and non-government customers using ADFS will leverage existing user accounts for their internal domain infrastructures and will not need to distribute additional authenticators specific to Office 365 MT.  Customers managing user accounts via the SUE portal will need to distribute unique Office 365 credentials.  For more information on managing passwords in SUE, see the following help article: http://office.microsoft.com/en-us/office365-suite-help/reset-a-user-s-password-HA102816058.aspx  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Smartcards are distributed by Microsoft's Global Security Account Management (GSAM) team. GSAM verifies as part of initial authenticator distribution the identity of the individual receiving the identifier by checking their US Government issued photo ID (e.g. driver's license or passport).  Initial service team domain passwords are distributed automatically by Microsoft account management tools, which identify and authenticate Office 365 MT administrators based on their CorpNet credentials before providing the password. Devices are identified during the provisioning process based on information provided by Azure; the domain joining process in Active Directory ensures that the correct identifier is assigned. |
| Part b | **Customer Responsibility:**  Office 365 MT customers are responsible for defining authenticator content requirements consistent with their organizational policies and requirements for their organizational users. Government and non-government customers using ADFS set their authenticator content requirements in their internal domain infrastructure - there are no separate requirements for Office 365 MT.  Customers managing users via SUE may set password requirements in the SUE portal. For more information on managing passwords via the SUE portal, please see the following instructional video: http://office.microsoft.com/en-us/office365-suite-help/manage-passwords-in-office-365-RZ104046885.aspx?CTT=5&origin=VA104058349  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Initial smartcard certificates are generated at the time of distribution. Recipients of a new smartcard are required to set a PIN immediately.  Service team domain account passwords are set randomly by Microsoft account management tools during account creation. Device authenticators are set automatically by Active Directory as part of the domain joining process. |
| Part c | **Customer Responsibility:**  Office 365 MT customers are responsible for ensuring that authenticators have sufficient strength for their intended use consistent with their organizational policies and requirements for their organizational users. Government and non-government customers using ADFS set their authenticator content requirements in their internal domain infrastructure - there are no separate requirements for Office 365 MT.  Customers not using ADFS who manage users via AAD may set password requirements via the SUE portal. For more information on managing passwords via the SUE portal, please see the following instructional video: http://office.microsoft.com/en-us/office365-suite-help/manage-passwords-in-office-365-RZ104046885.aspx?CTT=5&origin=VA104058349  **DNS, EXO, IP, WAC:**  Office 365 MT ensures that authenticators are sufficiently strong by configuring Active Directory such that passwords must comply with Windows strong password requirements and be at least 12 characters in length. Windows strong passwords must contain characters from at least three of these four categories:  • English lowercase  • English uppercase  • Numbers (0-9)  • Special characters  Device authenticators are set automatically by Active Directory as part of the domain joining process.  **Bing, Delve, MSTeams, OLM, OSI, SFB, SPO, SUE:**  Office 365 MT ensures that authenticators are sufficiently strong by configuring Active Directory or AAD and Torus such that passwords must comply with Windows strong password requirements and be at least 15 characters in length. Windows strong passwords must contain characters from at least three of these four categories:  • English lowercase  • English uppercase  • Numbers (0-9)  • Special characters  Device authenticators are set automatically by Active Directory as part of the domain joining process.  **SWE:**  Office 365 MT ensures that authenticators are sufficiently strong by configuring Active Directory such that passwords must comply with Windows strong password requirements and be at least 16 characters in length. Windows strong passwords must contain characters from at least three of these four categories:  • English lowercase  • English uppercase  • Numbers (0-9)  • Special characters  Device authenticators are set automatically by Active Directory as part of the domain joining process. |
| Part d | **Customer Responsibility:**  Office 365 MT customers are responsible for distributing authenticators, managing lost or damaged authenticators, and revoking authenticators in compliance with their organizational policies and requirements for their organizational users. Government and non-government customers using ADFS will leverage existing user accounts for their internal domain infrastructures and will not need to distribute additional authenticators specific to Office 365 MT.  Customers managing user accounts via the SUE portal will need to distribute unique Office 365 credentials. For more information on managing passwords via the SUE portal, see the following instructional video: http://office.microsoft.com/en-us/office365-suite-help/manage-passwords-in-office-365-RZ104046885.aspx?CTT=5&origin=VA104058349  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Microsoft's Global Security Account Management (GSAM) team has established and implemented procedures for handling smartcard distribution, for dealing with lost/compromised/damaged smartcards, and for revoking smartcard certificates. These procedures are available at the GSAM SharePoint site.  Smartcard distribution is described in part (a) of this control. If a card is reported lost or damaged, the certificates on the card are immediately revoked and a new card is issued. In other situations requiring revocation (personnel termination, for example), GSAM follows procedures for immediate certificate revocation and a new card is not issued.  Service team domain account passwords are set by Office 365 MT service team administrators. This process is followed for initial password distribution and if a password is forgotten. Passwords are not "revoked"; rather, the account is disabled in situations requiring revocation.  Device authenticators are automatically managed by Active Directory.  Additionally, for OLM, remote access to the Linux servers is through a SSH gateway tied to Torus and JIT. An engineer elevates against Torus using a Yubikey with PIN+touch policy. Elevation request parameters are signed with Yubikey’s private key to guarantee that request came from the engineer who owns Yubikey. After approval is granted, Torus sends the required authentication certificates to the engineer, and the certificate is tied to the YubiKey. Using the YubiKey with PIN+touch policy and certificates, the engineer then accesses the gateway. Remote access to the PAVC scanner is done using CJIS and RDP. |
| Part e | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Default authenticators are deleted, renamed or changed (in the case of passwords), or disabled prior to information system installation as part of automated deployment processes. |
| Part f | **Customer Responsibility:**  Office 365 MT customers are responsible for managing authenticator minimum and maximum lifetimes in compliance with their organizational policies and requirements for their organizational users. Government and non-government customers using ADFS will leverage existing user accounts for their internal domain infrastructures and will not need to manage minimum and maximum lifetimes for authenticators specific to Office 365 MT.  Customers not using ADFS who manage users in Azure Active Directory (AAD) will need to configure password lifetimes via the SUE portal. For more information on managing passwords via the SUE portal, see the following instructional video: http://office.microsoft.com/en-us/office365-suite-help/manage-passwords-in-office-365-RZ104046885.aspx?CTT=5&origin=VA104058349  **DNS:**  In accordance with the Office 365 Information Security Policy, authenticator requirements for Office 365 MT services include the following:   * Enforce password history = 24 passwords remembered * Maximum password age: Microsoft has documented the decision to allow the maximum password age of 70 days for DNS in the decision log “Guidance on FedRAMP Control IA-05(g)” * Minimum password age = 0 days   These requirements are enforced by domain level policy for the production environment. Microsoft has documented the decision to set the minimum password age to 0 days in the Decision Log “Guidance on FedRAMP Control IA-5(1)(d)”.  **Bing, Delve, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  In accordance with the Office 365 Information Security Policy and associated standards, authenticator requirements for Office 365 MT services include the following:  • Enforce password history = 24 passwords remembered  • Maximum password age = 60 days  • Minimum password age = 0 days  These requirements are enforced by domain level policy for the production environment. Microsoft has documented the decision to set the minimum password age to 0 days in the Decision Log “Guidance on FedRAMP Control IA-5(1)(d)”. |
| Part g | **Customer Responsibility:**  Office 365 MT customers are responsible for refreshing authenticators in compliance with their organizational policies and requirements for their organizational users. Government and non-government customers using ADFS will leverage existing user accounts for their internal domain infrastructures and will not need to refresh separate authenticators specific to Office 365 MT.  Customers not using ADFS will need to set credential refresh rules via the SUE portal. For more information on managing passwords via the SUE portal, see the following instructional video: http://office.microsoft.com/en-us/office365-suite-help/manage-passwords-in-office-365-RZ104046885.aspx?CTT=5&origin=VA104058349  **Bing, Delve, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Maximum password age is 60 days.  **DNS:**  Microsoft has documented the decision to allow the maximum password age of 70 days for DNS in the decision log “Guidance on FedRAMP Control IA-05(g)”. |
| Part h | **Customer Responsibility:**  Office 365 MT customers using ADFS to manage accounts for their organizational users are responsible for securing their internal Active Directory infrastructure as well as their ADFS servers to prevent unauthorized disclosure and modification of authenticators for their users.  Customers using the SUE portal to manage accounts inherit protections specific to this requirement from Azure Active Directory (AAD). AAD stores and transmits passwords as hashes of a one-way function using the same process as the Windows operating system.  For more information on how passwords are stored in Windows environments, see TechNet article 994558: http://technet.microsoft.com/en-us/library/hh994558(v=ws.10).aspx  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Passwords are encrypted and stored in the Active Directory database. At any point where password entry is required, Windows Security Services requires that the characters typed in are obfuscated from view. This is enforced as a group policy object within the operating system.  For more information on how passwords are stored in Windows environments, see TechNet article 994558: http://technet.microsoft.com/en-us/library/hh994558(v=ws.10).aspx |
| Part i | **Customer Responsibility:**  Office 365 MT customers are responsible for ensuring that their organizational users take measures to safeguard authenticators consistent with their organizational requirements.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  As established by the Office 365 Information Security Policy and associated standards, passwords must not be shared or revealed to anyone other than the authorized Office 365 MT user and must be encrypted when stored. Additionally, passwords 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 in 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. All personnel are required to report the loss or theft of smartcards immediately. |
| Part j | **Customer Responsibility:**  Office 365 MT customers are responsible for ensuring that authenticators for group/role accounts are changed when membership to those accounts changes.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT does not use group accounts. |

#### IA-5 (1) Control Enhancement (L) (M)

The information system, for password-based authentication:

1. Enforces minimum password complexity of [FedRAMP Assignment: case sensitive, minimum of twelve (12) characters, and at least one (1) each of upper-case letters, lower-case letters, numbers, and special characters];
2. Enforces at least the following number of changed characters when new passwords are created: [FedRAMP Assignment: at least one (1)];
3. Stores and transmits only cryptographically-protected passwords;
4. Enforces password minimum and maximum lifetime restrictions of [FedRAMP Assignment: one (1) day minimum, sixty (60) day maximum];
5. Prohibits password reuse for [FedRAMP Assignment: twenty-four (24)] generations; and
6. Allows the use of a temporary password for system logons with an immediate change to a permanent password.

| IA-5 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Customer Administrator, Service Engineer Operations | |
| Parameter IA-05(1)(a):  at least 12 characters and meeting Windows strong password requirements | |
| Parameter IA-05(1)(b):  at least one | |
| Parameter IA-05(1)(d):  0 days minimum, 60 days maximum | |
| Parameter IA-05(1)(e):  24 | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| IA-5 (1) - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility:**  Office 365 MT customers are responsible for enforcing password complexity in compliance with their organizational policies and requirements for their organizational users. Government and non-government customers using ADFS will leverage existing user accounts for their internal domain infrastructures and will use the same password complexity requirements to access Office 365 MT.  Customers managing user accounts in AAD via the SUE portal will need to configure password complexity requirements in the SUE portal. For more information on managing passwords via the SUE portal, see the following instructional video: http://office.microsoft.com/en-us/office365-suite-help/manage-passwords-in-office-365-RZ104046885.aspx?CTT=5&origin=VA104058349  **DNS, EXO, IP, WAC:**  Office 365 MT ensures that authenticators are sufficiently strong by configuring Active Directory or Azure Active Directory such that passwords must comply with Windows strong password requirements and be at least 12 characters in length. Windows strong passwords must contain characters from at least three of these four categories:  • English lowercase  • English uppercase  • Numbers (0-9)  • Special characters  These requirements are enforced by domain level policy for the production environment. Device authenticators are set automatically by Active Directory as part of the domain joining process.  **Bing, Delve, MSTeams, OLM, OSI, SFB, SPO, SUE:**  Office 365 MT ensures that authenticators are sufficiently strong by configuring Active Directory such that passwords must comply with Windows strong password requirements and be at least 14 characters in length. Windows strong passwords must contain characters from at least three of these four categories:  • English lowercase  • English uppercase  • Numbers (0-9)  • Special characters  These requirements are enforced by domain level policy for the production environment. Device authenticators are set automatically by Active Directory as part of the domain joining process.  **SWE:**  Office 365 MT ensures that authenticators are sufficiently strong by configuring Active Directory such that passwords must comply with Windows strong password requirements and be at least 16 characters in length. Windows strong passwords must contain characters from at least three of these four categories:  • English lowercase  • English uppercase  • Numbers (0-9)  • Special characters  These requirements are enforced by domain level policy for the production environment.  Device authenticators are set automatically by Active Directory as part of the domain joining process. |
| Part b | **Customer Responsibility:**  Office 365 MT customers are responsible for character changes in compliance with their organizational policies and requirements for their organizational users. Government and non-government customers using ADFS will leverage existing user accounts for their internal domain infrastructures and will use the same password change requirements to access Office 365 MT.  Customers managing user accounts in Azure Active Directory (AAD) via the SUE portal are not able to automatically enforce password changes that exceed a single character; it is not possible for the server to evaluate the number of characters changed in a password absent reversible password storage, which Office 365 MT does not support - reversible password storage significantly decreases the security of passwords. In this instance password change requirements will need to be enforced via policy and training of organizational users.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  For password-based authentication, Office 365 MT enforces at least a one-character change when new passwords are created. OLM engineers authenticate to Linux gateway servers using certificate based authentication, as discussed above. This requirement is enforced by domain level policy for the production environment. |
| Part c | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  For password-based authentication, Office 365 MT stores and transmits only encrypted representations of passwords. Passwords are stored and transmitted using a one-way function to hash the password value. These hashes are not reversible and the actual password is never stored or transmitted in clear text. Password transmission sessions are themselves encrypted using TLS. OLM engineers authenticate to Linux gateway servers using certificate based authentication, as discussed above. |
| Part d | **Customer Responsibility:**  Office 365 MT customers are responsible for managing authenticator minimum and maximum lifetimes in compliance with their organizational policies and requirements for their organizational users. Government and non-government customers using ADFS will leverage existing user accounts for their internal domain infrastructures and will not need to manage minimum and maximum lifetimes for authenticators specific to Office 365 MT.  Customers managing user accounts in Azure Active Directory (AAD) via the SUE portal will need to configure password lifetimes via the SUE portal. For more information on managing passwords via the SUE portal, see the following instructional video: http://office.microsoft.com/en-us/office365-suite-help/manage-passwords-in-office-365-RZ104046885.aspx?CTT=5&origin=VA104058349  **DNS:**  In accordance with the Office 365 Information Security Policy, authenticator requirements for Office 365 MT services include the following:   * Enforce password history = 24 passwords remembered * Maximum password age: Microsoft has documented the decision to allow the maximum password age of 70 days for DNS in the decision log “Guidance on FedRAMP Control IA-05(g)” * Minimum password age = 0 days   These requirements are enforced by domain level policy for the production environment. Microsoft has documented the decision to set the minimum password age to 0 days in the Decision Log “Guidance on FedRAMP Control IA-5(1)(d)”.  **Bing, Delve, EXO, IP, MSTeams, OSI, SFB, SPO, SUE, SWE, WAC:**  In accordance with the Office 365 Information Security Policy, authenticator requirements for Office 365 MT services include the following:   * Enforce password history = 24 passwords remembered * Maximum password age = 60 days * Minimum password age = 0 days   These requirements are enforced by domain level policy for the production environment. Microsoft has documented the decision to set the minimum password age to 0 days in the Decision Log “Guidance on FedRAMP Control IA-5(1)(d)”.  **OLM**:  Office 365 engineers authenticate to Linux gateway servers using certificate based authentication, as discussed above. |
| Part e | **Customer Responsibility:**  Office 365 MT customers are responsible for managing password reuse generations in compliance with their organizational policies and requirements for their organizational users. Government and non-government customers using ADFS will leverage existing user accounts for their internal domain infrastructures and will not need to manage password reuse generations for authenticators specific to Office 365 MT.  Non-government customers managing user accounts in Azure Active Directory (AAD) via the SUE portal will need to configure password reuse generations via the SUE portal. For more information on managing passwords via the SUE portal, see the following instructional video: http://office.microsoft.com/en-us/office365-suite-help/manage-passwords-in-office-365-RZ104046885.aspx?CTT=5&origin=VA104058349  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  For password-based authentication, Office 365 prohibits password reuse for 24 generations. OLM engineers authenticate to Linux gateway servers using certificate based authentication, as discussed above. |
| Part f | **Customer Responsibility:**  Government and non-government customers using ADFS are responsible for requiring a user to change their password immediately upon login when a temporary password is used.  For non-government customers managing user accounts in Azure Active Directory (AAD) via the SUE portal, AAD will require a temporary password to be changed the first time it is used.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT service team Active Directory or Azure Active Directory domains require service team users to change temporary passwords immediately upon login. |

#### IA-5 (2) Control Enhancement (M) (H)

The information system, for PKI-based authentication:

1. Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information;
2. Enforces authorized access to the corresponding private key;
3. Maps the authenticated identity to the account of the individual or group; and
4. Implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.

| IA-5 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: Customer Administrator, Office 365 Security Manager, 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| IA-5 (2) - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility:**  Government and non-government customers using ADFS to manage accounts for their organizational users, and using PKI in their authentication processes, are responsible for validating certificates by constructing a certification path with status information to an accepted trust anchor. ADFS uses the same certification process as the organization's internal domain authentication processes and is not unique to Office 365 MT.  Non-government customers managing accounts via the SUE portal do not use PKI-based authentication.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Microsoft’s corporate PKI has been established to provide a variety of digital certificate services to support operations for Office 365 MT and for the Microsoft Corporation. The Microsoft Corporate PKI functions as the Certificate Authority (CA) and Registration Authority and provides directory services to manage keys and certificates.  Office 365 MT uses role-based certificates to manage access to administrative applications. The certificates are signed by an internal Microsoft CA and are validated against that CA's public key. Office 365 MT also checks certificates against certificate revocation lists. |
| Part b | **Customer Responsibility:**  Office 365 MT customers, Government and non-government, using ADFS to manage accounts for their organizational users, and using PKI in their authentication processes, are responsible for enforcing access to the corresponding private key. ADFS uses the same certification process as the organization's internal domain authentication processes and is not unique to Office 365 MT.  Non-government customers managing accounts via the SUE portal do not use PKI-based authentication.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Microsoft protects its private keys by enforcing appropriate/authorized access restrictions. In accordance with the Public Key Infrastructure Operational Security Standard, Office 365 leverages the cryptographic capabilities that are directly a part of the operating system for certificates and authentication mechanisms (e.g. Kerberos). These cryptographic modules have been certified by NIST as being FIPS 140-2 complaint. Any time cryptographic capabilities are employed to protect the confidentiality, integrity, or availability of data within Office 365 MT, the modules and ciphers used are FIPS 140-2 compliant. For additional information on how cryptographic modules are employed in Microsoft products, see TechNet article cc750357: http://technet.microsoft.com/en-us/library/cc750357.aspx |
| Part c | **Customer Responsibility:**  Office 365 MT customers, Government and non-government, using ADFS to manage accounts for their organizational users, and using PKI in their authentication processes, are responsible for mapping the authenticated identity to a user account. ADFS uses the same certification process as the organization's internal domain authentication processes and is not unique to Office 365 MT.  Non-government customers managing accounts via the SUE portal do not use PKI-based authentication.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Microsoft smartcard certificates include user information for the purposes of mapping the smartcard identity to the active directory account of the card holder. |
| Part d | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT domain controllers cache revocation data and make it available to Office 365 MT servers if the primary revocation lists are unavailable. |

#### IA-5 (3) Control Enhancement (M) (H)

The organization requires that the registration process to receive [FedRAMP Assignment: All hardware/biometric (multifactor authenticators] be conducted [FedRAMP Selection: in person] before [Assignment: organization-defined registration authority] with authorization by [Assignment: organization-defined personnel or roles].

| IA-05(3) | Control Summary Information |
| --- | --- |
| Responsible Role: MSIT | |
| Parameter IA-05(3):  1. smartcards; 2. in person or via FedEx; 3. Microsoft GSAM; 4. account managers identified in Microsoft account management tools | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| IA-05(3) - What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility:**  Office 365 MT customers are responsible for registering authenticators in compliance with their organizational policies and requirements for their organizational users. Government and non-government customers using ADFS will leverage existing user accounts for their internal domain infrastructures and will not need to register additional authenticators specific to Office 365 MT.  Non-government customers managing user accounts in Azure Active Directory (AAD) via the SUE portal will need to register unique Office 365 authenticators. For more information on managing passwords via the SUE portal, see the following instructional video: http://office.microsoft.com/en-us/office365-suite-help/manage-passwords-in-office-365-RZ104046885.aspx?CTT=5&origin=VA104058349  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  As part of the Office 365 MT registration process, Microsoft requires Microsoft administrators within Office 365 MT to obtain their smartcard in person or via FedEx mail.  Cards are shipped via FedEx in a deactivated state and cannot be used until they are activated. A note is added to the cardkey account confirming the shipping number for tracking. Shipments require an adult signature for delivery. Badges are not activated until MSIT receives a confirmation email from the Microsoft user, user's manager, AAM, or Security. |

#### IA-5 (4) Control Enhancement (M)

The organization employs automated tools to determine if password authenticators are sufficiently strong to satisfy [*Assignment: organization-defined requirements*].

IA-5(4) Additional FedRAMP Requirements and Guidance:

Guidance: If automated mechanisms which enforce password authenticator strength at creation are not used, automated mechanisms must be used to audit strength of created password authenticators.

| IA-05(4) | Control Summary Information |
| --- | --- |
| Responsible Role: MSIT | |
| Parameter IA-05(4):  password length, complexity, rotation and lifetime restrictions as enforced by AD group policy | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| IA-05(4) - What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility:**  Office 365 MT government and non-government customers using ADFS are responsible for utilizing automated mechanisms to determine if password authenticators are sufficiently strong.  Non-government customers managing accounts in Azure Active Directory (AAD) via SUE will inherit default password strength policy enforcement from AAD. Please see the following article for more information:  http://technet.microsoft.com/en-us/library/jj943764.aspx  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Active Directory, or Azure Active Directory, is the automated tool employed by Office 365 MT to determine if password authenticators are sufficiently strong to satisfy the password length, complexity, rotation and lifetime restrictions placed on the Office 365 MT environment. Active Directory ensures that the password authenticator strength at creation is sufficient. |

#### IA-5 (6) Control Enhancement (M) (H)

The organization protects authenticators commensurate with the security category of the information to which use of the authenticator permits access.

| IA-05(6) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| IA-05(6) - What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility:**  Government and non-government customers using ADFS to manage accounts for their organizational users are responsible for securing their internal Active Directory (AD) infrastructure as well as their ADFS servers to prevent unauthorized disclosure and modification of authenticators for their users.  Non-government customers using the SUE portal to manage accounts inherit protections specific to this requirement from Azure Active Directory (AAD). AAD stores and transmits passwords as hashes of a one-way function using the same process as the Windows operating system. For more information on how passwords are stored in Windows environments, see TechNet article 994558: http://technet.microsoft.com/en-us/library/hh994558(v=ws.10).aspx  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT authenticators are stored within Office 365 MT systems, and are protected at least equivalently to all other information within Office 365 MT major applications. |

#### IA-5 (7) Control Enhancement (M) (H)

The organization ensures that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys.

| IA-05(7) | Control Summary Information |
| --- | --- |
| Responsible Role: 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| IA-05(7) - What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility:**  Office 365 MT government and non-government customers are responsible for ensuring that they do not store authenticators for their organizational users in scripts or function keys or embed them in applications.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT 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. |

#### IA-5 (11) Control Enhancement (L) (M) (H)

The information system, for hardware token-based authentication, employs mechanisms that satisfy [Assignment: organization-defined token quality requirements].

| IA-05(11) | Control Summary Information |
| --- | --- |
| Responsible Role: MSIT | |
| Parameter IA-05(11):  eAuth Level 3 and FIPS 140-2 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| IA-05(11) - What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility:**  Office 365 MT government and non-government customers utilizing hardware token-based authentication are responsible for employing mechanisms that satisfy their token quality requirements.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT uses multifactor authentication for network access by Office 365 MT personnel through the use of eAuth Level 4 and FIPS 140-2 compliant Gemalto smartcards or approved eAuth Level 4 and FIPS 140-2 compliant TPM modules. OLM also uses YubiKeys with RSA certificates. |

### IA-6 Authenticator Feedback (L) (M) (H)

The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

| IA-06 | Control Summary Information |
| --- | --- |
| Responsible Role: None – Automated | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| IA-06 - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT implements authenticator feedback through the use of the built-in operating system security controls that protect passwords when authenticating to system components. Passwords are obfuscated during the login process. No feedback is provided during the authentication process that could lead to potential exploitation by unauthorized users. |

### IA-7 Cryptographic Module Authentication (L) (M) (H)

The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

| IA-07 | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| IA-07 - What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility:**  Government and non-Government customers do not have access to request cryptographic certificates from Office 365 MT. If they require cryptographic certificates, they must follow their organizational procedures to procure certificates from a valid certificate authority.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT implements FIPS 140-2 compliant encryption mechanisms on all communications between partners and between customers using cryptographic certificates issued by SSLAdmin which are anchored to the Microsoft Root Certificate Authority. In this implementation, the Microsoft Root Certificate Authority is the cryptographic module for Office 365 MT. In order to request a cryptographic certificate, an Office 365 MT administrator must be authenticated to the MSIT managed corporate network. The Office 365 MT administrator navigates to the internal Microsoft site http://ssladmin to request a certificate. The request is routed to the administrator’s manager for approval. Once the certificate is issued, the administrator uses two factor authentication to access Office 365 MT servers 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. Office 365 MT has an existing ISA with MSIT to provide this service. |

### IA-8 Identification and Authentication (Non-Organizational Users) (L) (M) (H)

The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).

| IA-08 | Control Summary Information |
| --- | --- |
| Responsible Role: Customer Administrator | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| IA-08 - What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility:**  Office 365 MT customers are responsible for determining users who have access to their information system. Thus, the responsibility is incumbent upon the customer to uniquely identify and authenticate non-organizational users (or processes acting on behalf of non-organizational users) who should have system access.  The government customer can invite guests and non-organizational users to SharePoint Online, Skype for Business, and MSTeams but the guest must either authenticate with a LiveID (in the case of SharePoint Online) or be authorized/admitted to the session by the credentialed government customer user (in the case of Skype for Business). It is the responsibility of the customer to follow their own Rules of Behavior and policies around inviting guests to their systems.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT does not allow any non-organizational users to authenticate to production systems. Customer users are considered organizational and are covered via IA-2.  If government customers decide to allow access to non-organizational users (or processes acting on behalf of a non-organizational user), they must ensure that such users or processes are uniquely identified and authenticated using credentials that meet or exceed the set of minimum federal government-wide technical, security, privacy, and organizational requirements. |

#### IA-8 (1) Control Enhancement (L) (M) (H)

The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials from other federal agencies.

| IA-08(1) | Control Summary Information |
| --- | --- |
| Responsible Role: Customer Administrator | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| IA-08(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.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT does not utilize Personal Identity Verification (PIV) credentials for service team users. PIV cards are not available to Office 365 MT service team personnel. Government customers are permitted to federate their accounts and are therefore responsible for implementing authentication access control systems that accept and electronically verify Personal Identity Verification (PIV) credentials issued to other federal agencies. |

#### IA-8 (2) Control Enhancement (L) (M) (H)

The information system accepts only FICAM-approved third-party credentials.

| IA-08(2) | Control Summary Information |
| --- | --- |
| Responsible Role: Customer Administrator | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| IA-08(2) - What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility:**  Government customers using ADFS are responsible for accepting and electronically verifying FICAM-approved third-party credentials. Government customers are permitted to federate their accounts and are therefore responsible for implementing authentication mechanisms that accept only FICAM-approved third-party credentials.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT does not accept or process any government customer credentials.  Office 365 MT does not utilize or support FICAM-approved third-party credentials for service team users. If government customers decide to allow access to non-organizational users, they must authenticate using FICAM-approved third-party credentials. Government customers are responsible for ensuring that approved third-party credentials meet or exceed the set of minimum federal government-wide technical, security, privacy, and organizational requirements. |

#### IA-8 (3) Control Enhancement (L) (M) (H)

The organization employs only FICAM-approved information system components in [Assignment: organization-defined information systems] to accept third-party credentials.

| IA-08(3) | Control Summary Information |
| --- | --- |
| Responsible Role: Customer Administrator | |
| Parameter IA-08(3):  Office 365 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| IA-08(3) - What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility:**  Government customers using ADFS are responsible for employing only FICAM-approved information system components to accept third-party credentials.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT does not accept or process any government customer credentials.  Office 365 MT does not utilize or support FICAM-approved third-party credentials for service team users. . If government customers decide to allow access to non-organizational users, they must accept only FICAM-approved third-party credentials using FICAM-approved information system components. Government customers are permitted to federate their accounts and are therefore responsible for ensuring that approved third-party credentials meet or exceed the set of minimum federal government-wide technical, security, privacy, and organizational requirements |

#### IA-8 (4) Control Enhancement (L) (M) (H)

The information system conforms to FICAM-issued profiles.

| IA-08(4) | Control Summary Information |
| --- | --- |
| Responsible Role: Customer Administrator | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| IA-08(4) - What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility:**  Government customers using ADFS are responsible for conforming to FICAM-issued profiles.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT does not utilize or support FICAM-approved third-party credentials for service team users. If government customers decide to allow access to non-organizational users, they must accept only FICAM-approved third-party credentials using FICAM-issued implementation profiles of approved authentication protocols. |

* 1. Incident Response (IR)

### IR-1 Incident Response Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:

An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and

Reviews and updates the current:

Incident response policy [FedRAMP Assignment: at least every three (3) years]; and

* 1. Incident response procedures [FedRAMP Assignment: at least annually].

| IR-1 | Control Summary Information |
| --- | --- |
| Responsible Role: BCM, Office 365 Trust Program Manager | |
| Parameter IR-01(a)(1):  Office 365 Security Manager | |
| Parameter IR-01(a)(2):  Office 365 Security Manager | |
| Parameter IR-01(b)(1):  annually | |
| Parameter IR-01(b)(2):  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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| IR-1 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Part 1:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Information Security Policy provides the overarching security guidance for Office 365 MT. This document addresses the purpose, scope, roles, responsibilities, compliance requirements, and required coordination among the various Microsoft organizations providing some level of support for the security of Office 365 MT. Policies are made available to roles providing support for incident response via SharePoint.  **Part 2:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Information Security Policy contains policies that must be met in the delivery and operation of Office 365 MT. Standards and Procedures to facilitate execution of these policies are documented in the Active Framework Controls, Office 365 Standard Operating Procedures (SOPs), and service team-specific SOPs These standards and procedures act as adjuncts to the security policy and provide implementation level requirements and details to carry out specific operational tasks. A detailed mapping of Office 365 Standards and Procedures to each control is available for review. Office 365 SOPs are distributed to roles providing support for incident response via SharePoint. |
| Part b | **Part 1:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Information Security Policy is reviewed and updated annually by the Office 365 Trust team.  **Part 2:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Standard Operating Procedures (SOPs) are reviewed and updated annually by the service teams and by Office 365 Trust. |

### IR-2 Incident Response Training (L) (M)

The organization provides incident response training to information system users consistent with assigned roles and responsibilities in accordance with NIST SP 800-53 Rev 4:

1. Within [Assignment: organization-defined time period] of assuming an incident response role or responsibility;

When required by information system changes; and

1. [FedRAMP Assignment: at least annually] thereafter.

| IR-2 | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager, Program Manager | |
| Parameter IR-02(a):  30 days | |
| Parameter IR-02(c):  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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| IR-2 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Security Incident & Response (Office 365 SIR) team provides centralized incident management and response for Office 365 MT. The Office 365 SIR team reviews the annual security training provided to all personnel with access to Office 365 MT to ensure that the training provides Office 365 MT personnel with the training necessary to detect potential incidents and how to hand off the investigation of those events to the Office 365 SIR team. Additionally, the Office 365 SIR team publishes the Office 365 Security Incident Response Plan (IR plan), and a wiki addressing Security Incident FAQs along with a "battlecard" with live incident instructions for Office 365 MT personnel. The wiki is located at the following link: https://microsoft.sharepoint.com/teams/o365sec/sir/SitePages/Home.aspx |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  As part of the management of Office 365 MT, the Office 365 Security Incident & Response (Office 365 SIR) team considers whether changes require additional incident response training. If so, the training is developed and provided to applicable personnel. |
| Part c | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT personnel with security-relevant roles will receive refresher training on incident response annually, as part of their regular security awareness training. Annual training is both initial training for new personnel and refresher training for current personnel. |

### IR-3 Incident Response Testing (M)

The organization tests the incident response capability for the information system [FedRAMP Assignment: at least annually] using [FedRAMP Assignment: see additional FedRAMP Requirements and Guidance] to determine the incident response effectiveness and documents the results.

IR-3 Additional FedRAMP Requirements and Guidance:

Requirements: The service provider defines tests and/or exercises in accordance with NIST Special Publication 800-61 (as amended). For JAB authorization, the service provider provides test plans to the JAB/AO annually. Test plans are approved and accepted by the JAB/AO prior to the test commencing.

| IR-03 | Control Summary Information |
| --- | --- |
| Responsible Role: BCM, Office 365 Security Manager, Program Manager | |
| Parameter IR-03:  1. annually; 2. penetration testing | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| IR-03 - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT tests the incident response capability by conducting a red-team penetration test of each service team annually. The results of the penetration test include an assessment of incident response effectiveness. |

#### IR-3 (2) Control Enhancement (M) (H)

The organization coordinates incident response testing with organizational elements responsible for related plans.

| IR-03(2) | Control Summary Information |
| --- | --- |
| Responsible Role: BCM, Office 365 Security Manager, Program Manager | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| IR-03(2) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Security Incident & Response (Office 365 SIR) team is responsible for coordinating incident handling activities with contingency planning activities managed by the Business Continuity Management team. If incidents or incident response tests trigger contingency plan activation criteria, contingency plans are followed in coordination with the incident response plan. |

### IR-4 Incident Handling (L) (M) (H)

The organization:

1. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery;
2. Coordinates incident handling activities with contingency planning activities; and
3. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.

IR-4 Additional FedRAMP Requirements and Guidance:

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 Role: BCM, Office 365 Security Manager, Program Manager | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| IR-4 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 MT service teams and Office 365 Security Incident & Response (SIR) team are responsible for managing the investigation and resolution of security incidents within Office 365 MT. The Office 365 Security team works with service teams to ensure that security incidents are contained and eradicated, and that recovery is completed.  While the specific activities to be performed will depend on the security incident itself, there are several critical activities that must be performed as part of the process of managing the security incident response. These activities include preparation; detection and analysis; containment; eradication; and recovery, and are detailed in the Office 365 Security Incident Response Plan. |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Security Incident & Response (Office 365 SIR) team is responsible for coordinating incident handling activities with contingency planning activities managed by the Business Continuity Management team. If incidents or incident response tests trigger contingency plan activation criteria, contingency plans are followed in coordination with the incident response plan. |
| Part c | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Security Incident & Response (Office 365 SIR) team is responsible for incorporating lessons learned from ongoing incident handling activities into procedures, training, and tests and exercises. A post-mortem of identified security incidents is conducted by Office 365 SIR. Any identified remediation items, including those impacting procedures, training, and tests and exercises, are tracked to resolution by the Office 365 SIR team manager. |

#### IR-4 (1) Control Enhancement (M) (H)

The organization employs automated mechanisms to support the incident handling process.

| IR-04(1) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager, 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| IR-04(1) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Security Incident & Response (SIR) team wiki is continually available to provide information about incident response processes to Office 365 MT service teams at the following link: https://microsoft.sharepoint.com/teams/o365sec/sir/SitePages/Home.aspx  Additionally, a ticketing tool is used by the Office 365 SIR team for documenting and tracking the stages of the incident response process. |

### IR-5 Incident Monitoring (L) (M) (H)

The organization tracks and documents information system security incidents.

| IR-05 | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager, 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| IR-05 - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT tracks incidents in Office Service Pulse (OSP) and documents security incidents using ticketing tools. Service teams also use those ticketing tools to notify the Office 365 Security Incident & Response (SIR) team of possible security incidents. Likewise, if the Office 365 SIR team identifies a possible incident by themselves, they open a ticket. If the incident is categorized as a security incident, the Office 365 SIR team tracks and documents the security incident response process using the ticket.  Tickets are used by the Office 365 SIR team and Service Team Engineering for reporting and tracking incidents and are retained indefinitely. As part of the incident management process, the Office 365 SIR team and Service Team Engineering pull, review and attach system logs to tickets according to their troubleshooting guides. These logs can contain and be used as evidence of a security incident. If it is determined additional evidence is required, the Office 365 SIR team will work with the service team and CELA to identify, collect and retain the evidence. |

### IR-6 Incident Reporting (L) (M) (H)

The organization:

1. Requires personnel to report suspected security incidents to the organizational incident response capability within [FedRAMP Assignment: US-CERT incident reporting timelines as specified in NIST SP800-61 (as amended)]; and
2. Reports security incident information to [Assignment: organization-defined authorities].

IR-6 Additional FedRAMP Requirements and Guidance

Requirement: Report security incident information according to FedRAMP Incident Communications Procedure.

| IR-6 | Control Summary Information |
| --- | --- |
| Responsible Role: BCM, Office 365 Security Manager, Service Engineer Operations | |
| Parameter IR-06(a):  a near real-time interval | |
| Parameter IR-06(b):  designated authorities (including US-CERT) as documented in designated authorities (including US-CERT) as documented in the Microsoft Office 365 Security Incident Response Plan | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| IR-6 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT service team personnel are required to report suspected security incidents to the Office 365 Security Incident & Response (SIR) team in near real time upon discovering a suspected security incident. See the Office 365 Security Incident Response Plan for more information. |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 SIR team reports incidents to designated authorities (including US-CERT) consistently with NIST SP 800-61 as documented in the Office 365 Security Incident Response Plan. |

#### IR-6 (1) Control Enhancement (M) (H)

The organization employs automated mechanisms to assist in the reporting of security incidents.

| IR-06(1) | Control Summary Information |
| --- | --- |
| Responsible Role: 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| IR-06(1) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Security Incident & Response (SIR) team uses ticketing tools as an automated mechanism to assist in the reporting of security incidents. Ticketing tools track the time elapsed and phases of the incident response process, helping to assure that incidents are reported in the timeframes required by IR-06 part b. |

### IR-7 Incident Response Assistance (L) (M) (H)

The organization provides an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.

| IR-07 | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager, 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| IR-07 - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Security Incident & Response (SIR) team provides the following website as a resource providing advice and assistance to Office 365 MT service team personnel: The page includes such information as:  • What are security incidents?  • How to identify such incidents  • How and Why to escalate the security incidents  • List of sample security incidents  • Who to contact in the event of a security incident  The contact information includes 24/7 on-call information, so there is always a resource available should Office 365 MT service teams need advice or assistance.  https://microsoft.sharepoint.com/teams/o365sec/sir/SitePages/Home.aspx |

#### IR-7 (1) Control Enhancement (M) (H)

The organization employs automated mechanisms to increase the availability of incident response related information and support.

| IR-07(1) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager, 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| IR-07(1) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Security Incident & Response (SIR) team provides the following website as a resource providing advice and assistance to Office 365 MT service team personnel: https://microsoft.sharepoint.com/teams/o365sec/sir/SitePages/Home.aspx  The page includes such information as:  • What are security incidents?  • How to identify such incidents  • How and Why to escalate the security incidents  • List of sample security incidents  • Who to contact in the event of a security incident  The contact information includes 24/7 on-call information, so there is always a resource available should Office 365 MT service teams need advice or assistance.  In the event that an incident impacted the availability of the Office 365 MT service, the current status and regular updates would be posted on the customer's Office 365 Service Health Dashboard, which is accessible via the customer’s administrative portal. For more information on the Office 365 Service Health Dashboard, visit: http://office.microsoft.com/en-us/office365-suite-help/view-the-status-of-your-services-HA102817837.aspx |

#### IR-7 (2) Control Enhancement (M) (H)

The organization:

1. Establishes a direct, cooperative relationship between its incident response capability and external providers of information system protection capability; and
2. Identifies organizational incident response team members to the external providers.

| IR-7 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: BCM, Program Manager | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| IR-7 (2) - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 Security Incident & Response (SIR) team maintains a list of incident response contacts for all partner organizations, including: peers internal to Microsoft, incident response POCs within partner organizations covered via ISAs, and customer incident response contacts. These partner organizations are also provided direct contact information for the Office 365 Security Incident & Response (SIR) Team. |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 Security Incident & Response (SIR) coordinates with peer teams inside MSIT and Azure as required for incidents internal to Microsoft. Coordination with external organizations is addressed in the ISAs with those groups for incidents that may cross organizational boundaries. Office 365 SIR coordinates with customers as required, consistent with the reporting timeframes outlined. All coordinated incidents are tracked by Office 365 SIR. |

### IR-8 Incident Response Plan (L) (M) (H)

The organization:

1. Develops 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; and
   8. Is reviewed and approved by [Assignment: organization-defined personnel or roles];
2. Distributes copies of the incident response plan to [FedRAMP Assignment: see additional FedRAMP Requirements and Guidance].

IR-8(b) Additional FedRAMP Requirements and Guidance:

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.

1. Reviews the incident response plan [FedRAMP Assignment: at least annually];
2. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing;
3. Communicates incident response plan changes to [FedRAMP Assignment: see additional FedRAMP Requirements and Guidance].

IR-8(e) Additional FedRAMP Requirements and Guidance:

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.

1. Protects the incident response plan from unauthorized disclosure and modification.

| IR-8 | Control Summary Information |
| --- | --- |
| Responsible Role: BCM, Program Manager | |
| Parameter IR-08(a)(8):  personnel identified in the incident response plan | |
| Parameter IR-08(b):  Service Engineer Operations, Office 365 Security Manager | |
| Parameter IR-08(c):  at least annually | |
| Parameter IR-08(e):  Service Engineer Operations, Office 365 Security Manager | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| IR-8 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Part 1:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT has developed and implemented an incident response plan through the adoption and implementation of the Office 365 Security Incident Response Plan. The document classifies incidents into the following four categories: false positive, security incident, potential security breach, and incident with privacy impact. The document also provides guidance for addressing each category of incident, provides a high-level approach for how the incident response capability fits into the overall organization, and describes the structure and organization of the incident response capabilities.  **Part 2:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT has developed and implemented an incident response plan through the adoption and implementation of the Office 365 Security Incident Response Plan. The document classifies incidents into the following four categories: false positive, security incident, potential security breach, and incident with privacy impact. The document also provides guidance for addressing each category of incident, provides a high-level approach for how the incident response capability fits into the overall organization, and describes the structure and organization of the incident response capabilities.  **Part 3:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT has developed and implemented an incident response plan through the adoption and implementation of the Office 365 Security Incident Response Plan. The document classifies incidents into the following four categories: false positive, security incident, potential security breach, and incident with privacy impact. The document also provides guidance for addressing each category of incident, provides a high-level approach for how the incident response capability fits into the overall organization, and describes the structure and organization of the incident response capabilities.  **Part 4:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The incident response plan establishes criteria for categorizing and reporting incidents (including false positives, security incidents, potential security breaches, and incidents with privacy impact) and explains the different phases of the incident response lifecycle. Details for each of the phases are explained in the plan, including SLAs which can be measured against to provide objective capability metrics. The plan 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 response capability.  As described in the incident response plan, incidents are owned by senior individuals. Those senior level individuals are appointed by management to drive remediation efforts and serve as liaisons for communications with the Communications Manager, the Office 365 Security Incident & Response (SIR) team, and other members of the response team.  **Part 5:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The incident response plan 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 into one of the following four categories: false positive, security incident, potential security breach, or incident with privacy impact. Security incidents are tracked in a ticketing system where they are categorized and assigned a severity rating. Security incident examples include, but are not limited to: e-mail viruses, rootkits, worms, denial of service attacks, unauthorized access, inappropriate use of network resources, and any other type of unauthorized, unacceptable, or unlawful activity involving Office 365 MT computer networks or data processing equipment. Compromise, disclosure, or use of information that occurs outside its intended purpose are also considered security incidents.  **Part 6:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The incident response plan establishes criteria for categorizing and reporting incidents (including false positives, security incidents, potential security breaches, and incidents with privacy impact) and explains the different phases of the incident response lifecycle. Details for each of the phases are explained in the plan, including Service Level Agreements (SLAs) which can be measured against to provide objective capability metrics. The plan 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 response capability.  **Part 7:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  As described in the incident response plan, incidents are owned by senior individuals. Those senior level individuals are appointed by management to drive remediation efforts and serve as liaisons for communications with the Communications Manager, the Office 365 Security Incident & Response (SIR) team, and other members of the response team.  **Part 8:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The incident response plan is reviewed and approved annually by an Incident Manager. |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The incident response plan is posted on the internal Office 365 SharePoint. The incident response plan is also communicated as a part of the annual security training provided for Office 365 personnel. When updates are made, the personnel filling roles and responsibilities named in the plan are notified via email. |
| Part c | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 Security Incident & Response team reviews and updates the incident response plan annually. |
| Part d | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  On a monthly basis, Office 365 reviews all impacting incidents for the previous month with the leadership/exec team. Impact and resolution of the incident and changes to the Office 365 Security Incident Response plan are covered.  For each incident, a formal Incident Report is produced by the service teams and augmented with the Office 365 Security Incident & Response (SIR) Team’s additions. These reports, which include lessons learned, are created for all events with a SEV 1 rating. For incidents of lesser severity, if there are significant lessons learned that have general applicability across Office 365, an incident report is created. The incident reports are maintained by Office 365 SIR and are provided to the relevant stakeholders for review.  Office 365 revises the incident response plan as necessary to address system and organizational changes or lessons learned from incidents and testing. |
| Part e | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The incident response plan is posted on the internal Office 365 SharePoint. The incident response plan is also communicated as a part of the annual compliance training provided for Office 365. A distribution list contains the names and contact information of all personnel responsible for incident response. This list is used to communicate that changes have been made to the incident response plan, to notify stakeholders of incidents, and to contact on-call personnel.  In addition to notifying incident response personnel within Office 365 MT of changes to the incident response plan, FedRAMP personnel are also notified. |
| Part f | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The incident response plan is posted on the internal Office 365 SharePoint. Office 365 uses SharePoint Online access control and version control functionality to protect the incident response plan from unauthorized disclosure and modification respectively. |

### IR-9 Information Spillage Response (M) (H)

The organization responds to information spills by:

1. Identifying the specific information involved in the information system contamination;
2. Alerting [Assignment: organization-defined personnel or roles] of the information spill using a method of communication not associated with the spill;
3. Isolating the contaminated information system or system component;
4. Eradicating the information from the contaminated information system or component;
5. Identifying other information systems or system components that may have been subsequently contaminated; and
6. Performing other [Assignment: organization-defined actions].

| IR-9 | Control Summary Information |
| --- | --- |
| Responsible Role: BCM, Customer Administrator, Program Manager | |
| Parameter IR-09(b):  Service Team Operations personnel | |
| Parameter IR-09(f):  Incident response 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| IR-9 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility:**  Customers are responsible for ensuring that information not authorized for storage or transmission within Office 365 MT is not stored on or transmitted via Office 365 MT services. If information is spilled, customer administrators can locate all instances of the spilled information using eDiscovery features of Office 365 and permanently delete the spilled information.  For information about eDiscovery in Office 365, please see: https://support.office.com/en-us/article/eDiscovery-in-Office-365-143b3ab8-8cb0-4036-a5fc-6536d837bfce?ui=en-US&rs=en-US&ad=US  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Self-service tools provided to customer administrators are available to them for use in an information spillage response.  Microsoft Support Services can be leveraged to assist a customer with activities, such as development of customer-specific procedures, policy implementation with regards to spillage and legal hold, modification of existing procedures to leverage the Office 365 self-service tools, and providing government "cleared" resources for spillage activities. Microsoft Support Services, by default, does not have any permissions within the Office 365 service. |
| Part b | **Customer Responsibility:**  Customers are responsible for alerting appropriate personnel or roles per their Information Spillage Policy using a method of communication not associated with the spill.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  See part a. |
| Part c | **Customer Responsibility:**  Customers are responsible for isolating the contaminated information system or system component using the self-service features provided in Office 365 MT.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  See part a. |
| Part d | **Customer Responsibility:**  Customers are responsible for eradicating the information from the contaminated information system or component using the self-service features provided in Office 365 MT.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  See part a. |
| Part e | **Customer Responsibility:**  Customers are responsible for identifying other information systems or system components that may have been subsequently contaminated using the self-service features provided in Office 365 MT.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  See part a. |
| Part f | **Customer Responsibility:**  Customers are responsible for developing and following procedures outlined in their Information Spillage Policy supported by the self-service features provided in Office 365 MT.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  See part a. |

#### IR-9 (1) Control Enhancement (M) (H)

The organization assigns [Assignment: organization-defined personnel or roles] with responsibility for responding to information spills.

| IR-09(1) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager | |
| Parameter IR-09(1):  Microsoft Support Services, if engaged by customer | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| IR-09(1) - What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility:**  Government customers are responsible for ensuring that information not authorized for storage or transmission within Office 365 MT is not stored on or transmitted via Office 365 MT services. If information is spilled, Office 365 MT offers customer administrators with appropriate roles the ability to quickly respond to a data spillage event, without needing to contact Microsoft for support by using self-service features. These features can be used to identify specific information involved in an information system contamination.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Self-service tools provided to customer administrators are available to them for use in an information spillage response.  Microsoft Support Services can be leveraged to assist a customer with activities, such as development of customer-specific procedures, policy implementation with regards to spillage and legal hold, modification of existing procedures to leverage the Office 365 self-service tools, and providing government "cleared" resources for spillage activities. Microsoft Support Services, by default, does not have any permissions within the Office 365 service. |

#### IR-9 (2) Control Enhancement (M)

The organization provides information spillage response training [Assignment: organization- defined frequency].

| IR-09(2) | Control Summary Information |
| --- | --- |
| Responsible Role: BCM, Program Manager | |
| Parameter IR-09(2):  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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| IR-09(2) - What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility:**  Government customers are responsible for training appropriate personnel or roles per their Information Spillage Policy using a method of communication not associated with the spill.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Microsoft Support Services can be leveraged to assist a customer with activities, such as development of customer-specific procedures, policy implementation with regards to spillage and legal hold, modification of existing procedures to leverage the Office 365 self-service tools, and providing government "cleared" resources for spillage activities. Microsoft Support Services, by default, does not have any permissions within the Office 365 service. |

#### IR-9 (3) Control Enhancement (M) (H)

The organization implements [Assignment: organization-defined procedures] to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions.

| IR-09(3) | Control Summary Information |
| --- | --- |
| Responsible Role: BCM, Program Manager | |
| Parameter IR-09(3):  system redundancy | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| IR-09(3) - What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility:**  Government customers are responsible for managing the status of their deployments during the information spillage event using the self-service features provided in Office 365.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Customer administrators utilizing Microsoft Support Services will not affect the ability of Office 365 MT administrators to carry out their assigned tasks. |

#### IR-9 (4) Control Enhancement (M) (H)

The organization employs [Assignment: organization-defined security safeguards] for personnel exposed to information not within assigned access authorizations.

| IR-09(4) | Control Summary Information |
| --- | --- |
| Responsible Role: BCM, Program Manager | |
| Parameter IR-09(4):  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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| IR-09(4) - What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility:**  Government customers are responsible for managing the status of their deployments during the information spillage event using the self-service features provided in Office 365 MT.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT service team administrators are required to take security awareness training and privileged access training annually. This training prepares them for exposure to information outside their assigned access authorization. |

* 1. Maintenance (MA)

### MA-1 System Maintenance Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls; and
2. Reviews and updates the current:
   1. System maintenance policy [FedRAMP Assignment: at least every three (3) years]; and
   2. System maintenance procedures [FedRAMP Assignment: at least annually].

| MA-1 | Control Summary Information |
| --- | --- |
| Responsible Role: Azure | |
| Parameter MA-01(a)(1):  Service Engineer Operations, Program Manager, Developer, Tester, Office 365 Trust Program Manager, Office 365 Security Manager, BCM | |
| Parameter MA-01(a)(2):  Service Engineer Operations, Program Manager, Developer, Tester, Office 365 Trust Program Manager, Office 365 Security Manager, BCM | |
| Parameter MA-01(b)(1):  annually | |
| Parameter MA-01(b)(2):  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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| MA-1 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Part 1:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Information Security Policy defines Office 365 MT policies. This document addresses the purpose, scope, roles, responsibilities, compliance requirements, and required coordination among the various Microsoft organizations providing some level of support for the security of Office 365 MT, which is inherited via an ISA from Azure. Policies are distributed to roles providing support for Office 365 MT system maintenance via SharePoint.  Standards and Procedures to facilitate execution of Office 365 MT policies are documented in the Active Framework Controls, Office 365 Standard Operating Procedures (SOPs), and service team-specific SOPs. These standards and procedures act as adjuncts to the security policy and provide implementation level requirements and details to carry out specific operational tasks. Office 365 SOPs are distributed to roles providing support for system maintenance via SharePoint.  Azure has implemented system maintenance policy and procedures in accordance with Microsoft’s Online Services: Physical and Environmental Security Standard. All Microsoft equipment and systems are regularly maintained in order to guarantee operational efficiency. Maintenance of any equipment or system must be performed in accordance with manufacturer’s recommendations, carried out by authorized personnel, and recorded in a maintenance ticket.  **Part 2:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  See MA-01(a)(1) |
| Part b | **Part 1:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Information Security Policy is reviewed and updated annually by the Office 365 Trust team. Azure policy and procedures are reviewed and updated annually by Azure.  **Part 2:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Standard Operating Procedures (SOPs) are reviewed and updated annually by the service teams and by Office 365 Trust. Azure policy and procedures are reviewed and updated annually by Azure. |

### MA-2 Controlled Maintenance (L) (M) (H)

The organization:

1. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements;
2. Approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;
3. Requires that [Assignment: organization-defined personnel or roles] explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs;
4. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs;
5. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and
6. Includes [Assignment: organization-defined maintenance-related information] in organizational maintenance records.

| MA-2 | Control Summary Information |
| --- | --- |
| Responsible Role: Azure | |
| Parameter MA-02(c):  data center management, property asset owners | |
| Parameter MA-02(f):  (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) | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| MA-2 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC**:  This control is inherited from Azure, which has a FedRAMP IaaS P-ATO (package ID F1209051525). |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC**:  This control is inherited from Azure, which has a FedRAMP IaaS P-ATO (package ID F1209051525). |
| Part c | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC**:  This control is inherited from Azure, which has a FedRAMP IaaS P-ATO (package ID F1209051525). |
| Part d | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC**:  This control is inherited from Azure, which has a FedRAMP IaaS P-ATO (package ID F1209051525). |
| Part e | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC**:  This control is inherited from Azure, which has a FedRAMP IaaS P-ATO (package ID F1209051525). |
| Part f | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC**:  This control is inherited from Azure, which has a FedRAMP IaaS P-ATO (package ID F1209051525). |

### MA-3 Maintenance Tools (M) (H)

The organization approves, controls, and monitors information system maintenance tools.

| MA-03 | Control Summary Information |
| --- | --- |
| Responsible Role: 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| MA-03 - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  iLO is a tool that is used to maintain and troubleshoot machines that have issues. The credentials required for authorization and authentication of iLO accounts are stored in each service team’s secret store (Central Admin, SCRAM, Grid Secrets, Secret Store or Azure Key Vault), and can only be accessed by approved service team engineers.  iLO accounts operate through a separate VLAN that requires 2FA for access. Access to these accounts are monitored. Secret retrieval from each team’s secret store is logged.  Other tools that may be used for system maintenance are inherited from Azure, which has a FedRAMP IaaS P-ATO (package ID F1209051525). |

#### MA-3 (1) Control Enhancement (M) (H)

The organization inspects the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.

| MA-03(1) | Control Summary Information |
| --- | --- |
| Responsible Role: 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| MA-03(1) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC**:  This control is inherited from Azure, which has a FedRAMP IaaS P-ATO (package ID F1209051525). |

#### MA-3 (2) Control Enhancement (M) (H)

The organization checks media containing diagnostic and test programs for malicious code before the media are used in the information system.

| MA-03(2) | Control Summary Information |
| --- | --- |
| Responsible Role: 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| MA-03(2) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC**:  This control is inherited from Azure, which has a FedRAMP IaaS P-ATO (package ID F1209051525). |

#### MA-3 (3) Control Enhancement (M) (H)

The organization prevents the unauthorized removal of maintenance equipment containing organizational information by:

1. Verifying that there is no organizational information contained on the equipment;
2. Sanitizing or destroying the equipment;
3. Retaining the equipment within the facility; or
4. Obtaining an exemption from [FedRAMP Assignment: the information owner explicitly authorizes removal of the equipment from the facility].

| MA-3 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: Azure | |
| Parameter MA-03(3)(d):  Data Center 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| MA-3 (3) - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC**:  This control is inherited from Azure, which has a FedRAMP IaaS P-ATO (package ID F1209051525). |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC**:  This control is inherited from Azure, which has a FedRAMP IaaS P-ATO (package ID F1209051525). |
| Part c | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC**:  This control is inherited from Azure, which has a FedRAMP IaaS P-ATO (package ID F1209051525). |
| Part d | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC**:  This control is inherited from Azure, which has a FedRAMP IaaS P-ATO (package ID F1209051525). |

### MA-4 Remote Maintenance (L) (M) (H)

The organization:

1. Approves and monitors nonlocal maintenance and diagnostic activities;
2. Allows the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system;
3. Employs strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions;
4. Maintains records for nonlocal maintenance and diagnostic activities; and
5. Terminates session and network connections when nonlocal maintenance is completed.

| MA-4 | Control Summary Information |
| --- | --- |
| Responsible Role: Program Manager | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| MA-4 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT personnel do not have local access to production equipment. The use of non-local maintenance and diagnostic tools is a business requirement for the system. All Office 365 MT access and non-local maintenance is performed through the remote access points as documented in AC-17. |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT personnel do not have local access to Office 365 MT production equipment. The use of non-local maintenance and diagnostic tools is a business requirement for the system. All Office 365 MT access and non-local maintenance is performed through the remote access points as documented in AC-17. |
| Part c | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  All Office 365 MT access and non-local maintenance is performed through the remote access points as documented in AC-17. Connection to the remote access point requires use of eAuth Level 4 and FIPS 140-2 compliant Gemalto smartcards or approved eAuth Level 4 and FIPS 140-2 compliant TPM modules. as described in IA-02(1). Connection from the remote access point to a particular server requires strong authentication as described in IA-05. All access to Office 365 is authorized, controlled, and approved as defined in AC-02. |
| Part d | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Service teams are required to have a documented change request logged in ticketing tools before performing maintenance on Office 365 MT. |
| Part e | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Service team personnel are trained as part of annual security training to terminate sessions when their work is completed. In addition, the remote access terminal server gateways are configured to disconnect network connections after 15 minutes of inactivity. |

#### MA-4 (2) Control Enhancement (M) (H)

The organization documents in the security plan for the information system, the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections.

| MA-04(2) | Control Summary Information |
| --- | --- |
| Responsible Role: Program Manager | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| MA-04(2) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT documents the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections in the Office 365 Information Security Policy and Office 365 MT Access Control (AC) Standard Operating Procedure (SOP). |

### MA-5 Maintenance Personnel (L) (M) (H)

The organization:

1. Establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel;
2. Ensures that non-escorted personnel performing maintenance on the information system have required access authorizations; and
3. Designates 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 Role: 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| MA-5 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC**:  This control is inherited from Azure, which has a FedRAMP IaaS P-ATO (package ID F1209051525). |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC**:  This control is inherited from Azure, which has a FedRAMP IaaS P-ATO (package ID F1209051525). |
| Part c | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC**:  This control is inherited from Azure, which has a FedRAMP IaaS P-ATO (package ID F1209051525). |

#### MA-5 (1) Control Enhancement (L) (M)

The organization:

1. Implements 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 information system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified;
   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 information system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured; and
2. Develops and implements alternate security safeguards in the event an information system component cannot be sanitized, removed, or disconnected from the system.

MA-5 (1) Additional FedRAMP Requirements and Guidance:

Requirement: Only MA-5 (1) (a) (1) is required by FedRAMP

| MA-5 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| MA-5 (1) - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Part 1:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC**:  This control is inherited from Azure, which has a FedRAMP IaaS P-ATO (package ID F1209051525).  **Part 2:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC**:  This control is inherited from Azure, which has a FedRAMP IaaS P-ATO (package ID F1209051525). |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC**:  This control is inherited from Azure, which has a FedRAMP IaaS P-ATO (package ID F1209051525). |

### MA-6 Timely Maintenance (M) (H)

The organization obtains maintenance support and/or spare parts for [Assignment: organization-defined information system components] within [Assignment: organization-defined time period] of failure.

| MA-06 | Control Summary Information |
| --- | --- |
| Responsible Role: Azure | |
| Parameter MA-06:  1. components documented in the CMMS tool; 2. Spare part/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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| MA-06 - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC**:  This control is inherited from Azure, which has a FedRAMP IaaS P-ATO (package ID F1209051525). |

* 1. Media Protection (MP)

### MP-1 Media Protection Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the media protection policy and associated media protection controls; and
2. Reviews and updates the current:
   1. Media protection policy [FedRAMP Assignment: at least every three (3) years]; and
   2. Media protection procedures [FedRAMP Assignment: at least annually].

| MP-1 | Control Summary Information |
| --- | --- |
| Responsible Role: Azure | |
| Parameter MP-01(a)(1):  personnel or roles responsible for media protection | |
| Parameter MP-01(a)(2):  personnel or roles responsible for media protection | |
| Parameter MP-01(b)(1):  annually | |
| Parameter MP-01(b)(2):  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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| MP-1 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Part 1:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The "Office 365 Information Security Policy" defines Office 365 MT policies. This document addresses the purpose, scope, roles, responsibilities, compliance requirements, and required coordination among the various Microsoft organizations providing some level of support for the security of Office 365 MT. Policies are distributed to personnel responsible for implementing media protection policies and procedures via SharePoint.  **Part 2:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Microsoft Enterprise Online Services Data Taxonomy (aka Asset Classification Standard) and O365 Data Handling Standard define appropriate handling and protection procedures of assets based on their classification. |
| Part b | **Part 1:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Information Security Policy is reviewed and updated annually. The Office 365 Information Security Policy is reviewed and approved annually.  **Part 2:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Microsoft Enterprise Online Services Data Taxonomy (aka Asset Classification Standard) and O365 Data Handling Standard are reviewed and approved annually. |

### MP-2 Media Access (L) (M)

The organization restricts access to [Assignment: organization-defined types of digital and/or non-digital media] to [Assignment: organization-defined personnel or roles].

| MP-02 | Control Summary Information |
| --- | --- |
| Responsible Role: Azure | |
| Parameter MP-02:  1. all types of digital and/or non-digital media containing information not cleared for public release; 2. personnel with duties requiring access to media containing non-public 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| MP-02 - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC**:  This control is inherited from Azure, which has a FedRAMP IaaS P-ATO (package ID F1209051525). |

### MP-3 Media Labeling (M) (H)

The organization:

1. Marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and
2. Exempts [FedRAMP Assignment: no removable media types] from marking as long as the media remain within [Assignment: organization-defined controlled areas].

MP-3(b) Additional FedRAMP Requirements and Guidance:

Guidance: Second parameter in MP-3(b)-2 is not applicable.

| MP-3 | Control Summary Information |
| --- | --- |
| Responsible Role: Azure | |
| Parameter MP-03(b):  1. no removable media types; 2. Office 365 data center premises | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| MP-3 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC**:  This control is inherited from Azure, which has a FedRAMP IaaS P-ATO (package ID F1209051525). |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC**:  This control is inherited from Azure, which has a FedRAMP IaaS P-ATO (package ID F1209051525). |

### MP-4 Media Storage (M) (H)

The organization:

1. Physically controls and securely stores [FedRAMP Assignment: [all types of digital and non-digital media with sensitive information]] within [FedRAMP Assignment: see additional FedRAMP requirements and guidance]; and

MP-4a Additional FedRAMP Requirements and Guidance:

Requirement: The service provider defines controlled areas within facilities where the information and information system reside.

1. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

| MP-4 | Control Summary Information |
| --- | --- |
| Responsible Role: Azure | |
| Parameter MP-04(a):  1. all types of digital and non-digital media with sensitive information; 2. in the production data center under the protection and monitoring from physical 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| MP-4 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC**:  This control is inherited from Azure, which has a FedRAMP IaaS P-ATO (package ID F1209051525). |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC**:  This control is inherited from Azure, which has a FedRAMP IaaS P-ATO (package ID F1209051525). |

### MP-5 Media Transport (M) (H)

The organization:

1. Protects and controls [FedRAMP Assignment: all media with sensitive information] during transport outside of controlled areas using [FedRAMP Assignment: for digital media, encryption using a FIPS 140-2 validated encryption module; for non-digital media, secured in locked container];

MP-5a Additional FedRAMP Requirements and Guidance:

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.

1. Maintains accountability for information system media during transport outside of controlled areas;

Documents activities associated with the transport of information system media; and

1. Restricts the activities associated with transport of information system media to authorized personnel.

| MP-5 | Control Summary Information |
| --- | --- |
| Responsible Role: Azure | |
| Parameter MP-05(a):  1. magnetic tapes, external/removable hard drives, diskettes, compact disks and digital video disks and non-digital media; 2. security functions are listed in Azure Physical Security Operations Standard Operating 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| MP-5 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC**:  This control is inherited from Azure, which has a FedRAMP IaaS P-ATO (package ID F1209051525). |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC**:  This control is inherited from Azure, which has a FedRAMP IaaS P-ATO (package ID F1209051525). |
| Part c | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC**:  This control is inherited from Azure, which has a FedRAMP IaaS P-ATO (package ID F1209051525). |
| Part d | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC**:  This control is inherited from Azure, which has a FedRAMP IaaS P-ATO (package ID F1209051525). |

#### MP-5 (4) Control Enhancement (M) (H)

The organization employs cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.

| MP-05(4) | Control Summary Information |
| --- | --- |
| Responsible Role: 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| MP-05(4) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC**:  This control is inherited from Azure, which has a FedRAMP IaaS P-ATO (package ID F1209051525). |

### MP-6 Media Sanitization and Disposal (L) (M)

The organization:

1. Sanitizes [Assignment: organization-defined information system media] prior to disposal, release out of organizational control, or release for reuse using [Assignment: organization-defined sanitization techniques and procedures] in accordance with applicable federal and organizational standards and policies; and
2. Employs sanitization mechanisms with strength and integrity commensurate with the classification or classification of the information.

| MP-6 | Control Summary Information |
| --- | --- |
| Responsible Role: Azure | |
| Parameter MP-06(a):  1. digital media, non-digital media is not used by Azure; 2. Digital media: Overwrite at least 3 times; Non-digital media: Burning, pulping, shredding, macerating | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| MP-6 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC**:  This control is inherited from Azure, which has a FedRAMP IaaS P-ATO (package ID F1209051525). |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC**:  This control is inherited from Azure, which has a FedRAMP IaaS P-ATO (package ID F1209051525). |

#### MP-6 (2) Control Enhancement (M)

The organization tests sanitization equipment and procedures [FedRAMP Assignment: at least annually] to verify that the intended sanitization is being achieved.

MP-6(2) Additional FedRAMP Requirements and Guidance:

Guidance: Equipment and procedures may be tested or evaluated for effectiveness.

| MP-06(2) | Control Summary Information |
| --- | --- |
| Responsible Role: Azure | |
| Parameter MP-06(2):  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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| MP-06(2) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC**:  This control is inherited from Azure, which has a FedRAMP IaaS P-ATO (package ID F1209051525). |

### MP-7 Media Use (L) (M) (H)

The organization [Selection: restricts; prohibits] the use of [Assignment: organization-defined types of information system media] on [Assignment: organization-defined information systems or system components] using [Assignment: organization-defined security safeguards].

| MP-07 | Control Summary Information |
| --- | --- |
| Responsible Role: Azure | |
| Parameter MP-07:  1. prohibits; 2. Azure defined information system media; 3. all information systems; 4. 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| MP-07 - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC**:  This control is inherited from Azure, which has a FedRAMP IaaS P-ATO (package ID F1209051525). |

#### MP-7 (1) Control Enhancement (M) (H)

The organization prohibits the use of portable storage devices in organizational information systems when such devices have no identifiable owner.

| MP-07(1) | Control Summary Information |
| --- | --- |
| Responsible Role: 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| MP-07(1) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC**:  This control is inherited from Azure, which has a FedRAMP IaaS P-ATO (package ID F1209051525). |

* 1. Physical and Environmental Protection (PE)

### PE-1 Physical and Environmental Protection Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:

A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls; and

Reviews and updates the current:

Physical and environmental protection policy [FedRAMP Assignment: at least every three (3) years]; and

* 1. Physical and environmental protection procedures [FedRAMP Assignment: at least annually].

| PE-1 | Control Summary Information |
| --- | --- |
| Responsible Role: Azure | |
| Parameter PE-01(a)(1):  Service Engineer Operations, Program Manager, Developer, Tester, Office 365 Trust Program Manager, Office 365 Security Manager, BCM | |
| Parameter PE-01(a)(2):  Service Engineer Operations, Program Manager, Developer, Tester, Office 365 Trust Program Manager, Office 365 Security Manager, BCM | |
| Parameter PE-01(b)(1):  annually | |
| Parameter PE-01(b)(2):  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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| PE-1 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Part 1:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Azure has implemented a physical and environmental policy and procedures to allow for the secure operation of Azure networks and data centers. The Office 365 Information Security Policy, Microsoft's Online Services Physical and Environmental Security Standard, and Enterprise Online Services Data Taxonomy are all maintained by Azure - Online Services Security & Compliance (OSSC) and reviewed and published annually. These documents address the purpose, scope, roles, responsibilities, compliance requirements, and required coordination among the various Azure organizations that provide physical and environmental support to Microsoft’s online services. The objective of the physical and environmental security policy in the Office 365 Information Security Policy is to prevent unauthorized access, damage or interference to Azure production facilities (data centers). Details on the physical and environmental security controls policy can be found in the Office 365 Information Security Policy.  The Office 365 Information Security Policy applies across the company to all information and processes used in the conduct of Microsoft business. All Microsoft employees and contingent staff are accountable and responsible for complying with these guiding principles within their designated roles.  Any exceptions or changes to the policy must be approved by the policy owner. Exceptions or changes to Standards which support this policy must be approved by the applicable Security Group.  Specific Security Groups (organizations which implement security programs that support this Policy) provide Standards with specific details for the satisfaction of the requirements in this policy. These Standards are followed within the scope of each Security Group’s authority.  The Office 365 Information Security Policy has been reviewed, approved, and is endorsed by Microsoft’s senior management.  The Online Services Information Security Policy is maintained and aligned with supporting corporate policies and functions such as, but not limited to, Human Resources, Corporate External & Legal Affairs, and Privacy.  Microsoft staff is required to strictly adhere to all applicable security policies, standards, regulations, and requirements.  Azure has developed the OSSC Physical Security Program Support SOP to properly implement Microsoft’s online services’ physical and environmental standards. The SOP provides details pertaining to the access control, Security Operations Center operations, audit and compliance, as well as the technology, applications and equipment employed at the data centers. OSSC Physical Security reviews the Microsoft’s Online Services Physical and Environmental Security Standards annually for any changes that require updates to the SOP.  The physical and environmental policy, standards and procedures are developed, disseminated, and reviewed annually within Azure. When updates are made, the new policy and standards are distributed to the physical security operations personnel through the Archer tool. Archer contains all data center policies and standards and can be accessed by the relevant teams operating Azure data centers. The SOPs for DCS are maintained on the DCS SharePoint (DCSWeb) sites.  **Part 2:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  See PE-1(a)(1) |
| Part b | **Part 1:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The physical and environmental protection policy and Asset Protection Standard are updated annually.  **Part 2:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  See PE-1(b)(1) |

### PE-2 Physical Access Authorizations (L) (M)

The organization:

1. Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides;

Issues authorization credentials for facility access;

Reviews the access list detailing authorized facility access by individuals [FedRAMP Assignment: at least annually]; and

Removes individuals from the facility access list when access is no longer required.

| PE-2 | Control Summary Information |
| --- | --- |
| Responsible Role: Azure | |
| Parameter PE-02(c):  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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| PE-2 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  This control is inherited from Azure which has a FedRAMP IaaS P-ATO (package ID F1209051525). |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  This control is inherited from Azure which has a FedRAMP IaaS P-ATO (package ID F1209051525). |
| Part c | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  This control is inherited from Azure which has a FedRAMP IaaS P-ATO (package ID F1209051525). |
| Part d | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  This control is inherited from Azure which has a FedRAMP IaaS P-ATO (package ID F1209051525). |

### PE-3 Physical Access Control (L) (M) (H)

The organization:

1. Enforces physical access authorizations at [Assignment: organization-defined entry/exit points to the facility where the information system resides] by:

Verifying individual access authorizations before granting access to the facility; and

Controlling ingress/egress to the facility using [FedRAMP Assignment: CSP defined physical access control systems/devices AND guards];

Maintains physical access audit logs for [Assignment: organization-defined entry/exit points];

Provides [Assignment: organization-defined security safeguards] to control access to areas within the facility officially designated as publicly accessible;

Escorts visitors and monitors visitor activity [FedRAMP Assignment: in all circumstances within restricted access area where the information system resides];

Secures keys, combinations, and other physical access devices;

1. Inventories [Assignment: organization-defined physical access devices] every [FedRAMP Assignment: at least annually]; and
2. Changes combinations and keys [FedRAMP Assignment: at least annually] and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.

| PE-3 | Control Summary Information |
| --- | --- |
| Responsible Role: Azure | |
| Parameter PE-03(a)(1):  all physical access points to the facility | |
| Parameter PE-03(a)(2):  1. all physical access points to the facility; 2. defined physical access control systems/devices | |
| Parameter PE-03(b):  all physical access points to the facility | |
| Parameter PE-03(c):  guards during working hours; guards, locks, and/or alarms during non-working hours | |
| Parameter PE-03(d):  in all circumstances within restricted access area where the information system resides | |
| Parameter PE-03(f):  1. keys, temporary access badges, access badge readers, and similar devices; 2. at least annually | |
| Parameter PE-03(g):  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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| PE-3 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Part 1:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  This control is inherited from Azure which has a FedRAMP IaaS P-ATO (package ID F1209051525).  **Part 2:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  This control is inherited from Azure which has a FedRAMP IaaS P-ATO (package ID F1209051525). |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  This control is inherited from Azure which has a FedRAMP IaaS P-ATO (package ID F1209051525). |
| Part c | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  This control is inherited from Azure which has a FedRAMP IaaS P-ATO (package ID F1209051525). |
| Part d | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  This control is inherited from Azure which has a FedRAMP IaaS P-ATO (package ID F1209051525). |
| Part e | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  This control is inherited from Azure which has a FedRAMP IaaS P-ATO (package ID F1209051525). |
| Part f | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  This control is inherited from Azure which has a FedRAMP IaaS P-ATO (package ID F1209051525). |
| Part g | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  This control is inherited from Azure which has a FedRAMP IaaS P-ATO (package ID F1209051525). |

### PE-4 Access Control for Transmission Medium (M) (H)

The organization controls physical access to [Assignment: organization-defined information system distribution and transmission lines] within organizational facilities using [Assignment: organization-defined security safeguards].

| PE-04 | Control Summary Information |
| --- | --- |
| Responsible Role: Azure | |
| Parameter PE-04:  1. all distribution and transmission lines; 2. 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| PE-04 - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  This control is inherited from Azure which has a FedRAMP IaaS P-ATO (package ID F1209051525). |

### PE-5 Access Control for Output Devices (M) (H)

The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.

| PE-05 | Control Summary Information |
| --- | --- |
| Responsible Role: 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| PE-05 - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  This control is inherited from Azure which has a FedRAMP IaaS P-ATO (package ID F1209051525). |

### PE-6 Monitoring Physical Access (L) (M) (H)

The organization:

1. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents;
2. Reviews physical access logs [FedRAMP Assignment: at least monthly] and upon occurrence of [Assignment: organization-defined events or potential indications of events]; and
3. Coordinates results of reviews and investigations with the organization’s incident response capability.

| PE-6 | Control Summary Information |
| --- | --- |
| Responsible Role: Azure | |
| Parameter PE-06(b):  1. at least every 30 days; 2. 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| PE-6 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  This control is inherited from Azure which has a FedRAMP IaaS P-ATO (package ID F1209051525). |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  This control is inherited from Azure which has a FedRAMP IaaS P-ATO (package ID F1209051525). |
| Part c | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  This control is inherited from Azure which has a FedRAMP IaaS P-ATO (package ID F1209051525). |

#### PE-6 (1) Control Enhancement (M) (H)

The organization monitors physical intrusion alarms and surveillance equipment.

| PE-06(1) | Control Summary Information |
| --- | --- |
| Responsible Role: 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| PE-06(1) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  This control is inherited from Azure which has a FedRAMP IaaS P-ATO (package ID F1209051525). |

### PE-8 Visitor Access Records (L) (M) (H)

The organization:

1. Maintains visitor access records to the facility where the information system resides for [FedRAMP Assignment: for a minimum of one (1) year]; and
2. Reviews visitor access records [FedRAMP Assignment: at least monthly]

| PE-8 | Control Summary Information |
| --- | --- |
| Responsible Role: Azure | |
| Parameter PE-08(a):  at least one year | |
| Parameter PE-08(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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| PE-8 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  This control is inherited from Azure which has a FedRAMP IaaS P-ATO (package ID F1209051525). |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  This control is inherited from Azure which has a FedRAMP IaaS P-ATO (package ID F1209051525). |

### PE-9 Power Equipment and Cabling (M) (H)

The organization protects power equipment and power cabling for the information system from damage and destruction.

| PE-9 | Control Summary Information |
| --- | --- |
| Responsible Role: 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| PE-9 - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  This control is inherited from Azure which has a FedRAMP IaaS P-ATO (package ID F1209051525). |

### PE-10 Emergency Shutoff (M) (H)

The organization:

1. Provides the capability of shutting off power to the information system or individual system components in emergency situations;
2. Places emergency shutoff switches or devices in [Assignment: organization-defined location by information system or system component] to facilitate safe and easy access for personnel; and
3. Protects emergency power shutoff capability from unauthorized activation.

| PE-10 | Control Summary Information |
| --- | --- |
| Responsible Role: Azure | |
| Parameter PE-10(b):  near exit doors | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| PE-10 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  This control is inherited from Azure which has a FedRAMP IaaS P-ATO (package ID F1209051525). |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  This control is inherited from Azure which has a FedRAMP IaaS P-ATO (package ID F1209051525). |
| Part c | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  This control is inherited from Azure which has a FedRAMP IaaS P-ATO (package ID F1209051525). |

### PE-11 Emergency Power (M) (H)

The organization provides a short-term uninterruptible power supply to facilitate [Selection (one or more): an orderly shutdown of the information system; transition of the information system to long-term alternate power] in the event of a primary power source loss.

| PE-11 | Control Summary Information |
| --- | --- |
| Responsible Role: Azure | |
| 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| PE-11 - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  This control is inherited from Azure which has a FedRAMP IaaS P-ATO (package ID F1209051525). |

### PE-12 Emergency Lighting (L) (M) (H)

The organization employs and maintains automatic emergency lighting for the information 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 Role: 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| PE-12 - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  This control is inherited from Azure which has a FedRAMP IaaS P-ATO (package ID F1209051525). |

### PE-13 Fire Protection (L) (M) (H)

The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.

| PE-13 | Control Summary Information |
| --- | --- |
| Responsible Role: 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| PE-13 - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  This control is inherited from Azure which has a FedRAMP IaaS P-ATO (package ID F1209051525). |

#### PE-13 (2) Control Enhancement (M) (H)

The organization employs fire suppression devices/systems for the information system that provide automatic notification of any activation [Assignment: organization-defined personnel or roles] and [Assignment: organization-defined emergency responders].

| PE-13(2) | Control Summary Information |
| --- | --- |
| Responsible Role: Azure | |
| Parameter PE-13(2):  1. local security staff and the Global Security Operations Center in Redmond; 2. 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| PE-13(2) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  This control is inherited from Azure which has a FedRAMP IaaS P-ATO (package ID F1209051525). |

#### PE-13 (3) Control Enhancement (M) (H)

The organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.

| PE-13(3) | Control Summary Information |
| --- | --- |
| Responsible Role: 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| PE-13(3) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  This control is inherited from Azure which has a FedRAMP IaaS P-ATO (package ID F1209051525). |

### PE-14 Temperature and Humidity Controls (L) (M) (H)

The organization:

1. Maintains temperature and humidity levels within the facility where the information system resides at [FedRAMP Assignment: consistent with American Society of Heating, Refrigerating and Air-conditioning Engineers (ASHRAE) document entitled "Thermal Guidelines for Data Processing Environments]; and

PE-14 (a) Additional FedRAMP Requirements and Guidance:   
Requirement: The service provider measures temperature at server inlets and humidity levels by dew point.

1. Monitors temperature and humidity levels [FedRAMP Assignment: continuously].

| PE-14 | Control Summary Information |
| --- | --- |
| Responsible Role: Azure | |
| Parameter PE-14(a):  Typically between 18 degrees Celsius to 27 degrees (64.4 degrees to 80.6 degrees Fahrenheit); humidity is measured by Relative Humidity Percentage Non-Condensing with the current range between 40% and 55%. | |
| Parameter PE-14(b):  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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| PE-14 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  This control is inherited from Azure which has a FedRAMP IaaS P-ATO (package ID F1209051525). |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  This control is inherited from Azure which has a FedRAMP IaaS P-ATO (package ID F1209051525). |

#### PE-14 (2) Control Enhancement (M) (H)

The organization employs temperature and humidity monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment.

| PE-14(2) | Control Summary Information |
| --- | --- |
| Responsible Role: 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| PE-14(2) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  This control is inherited from Azure which has a FedRAMP IaaS P-ATO (package ID F1209051525). |

### PE-15 Water Damage Protection (L) (M) (H)

The organization protects the information 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 Role: 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| PE-15 - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  This control is inherited from Azure which has a FedRAMP IaaS P-ATO (package ID F1209051525). |

### PE-16 Delivery and Removal (L) (M) (H)

The organization authorizes, monitors, and controls [FedRAMP Assignment: all information system components] entering and exiting the facility and maintains records of those items.

| PE-16 | Control Summary Information |
| --- | --- |
| Responsible Role: Azure | |
| Parameter PE-16:  all information 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| PE-16 - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  This control is inherited from Azure which has a FedRAMP IaaS P-ATO (package ID F1209051525). |

### PE-17 Alternate Work Site (M) (H)

The organization:

1. Employs [Assignment: organization-defined security controls] at alternate work sites;
2. Assesses as feasible, the effectiveness of security controls at alternate work sites; and
3. Provides a means for employees to communicate with information security personnel in case of security incidents or problems.

| PE-17 | Control Summary Information |
| --- | --- |
| Responsible Role: Azure | |
| Parameter PE-17(a):  all relevant controls are implemented at the primary 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| PE-17 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  This control is inherited from Azure which has a FedRAMP IaaS P-ATO (package ID F1209051525). |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  This control is inherited from Azure which has a FedRAMP IaaS P-ATO (package ID F1209051525). |
| Part c | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  This control is inherited from Azure which has a FedRAMP IaaS P-ATO (package ID F1209051525). |

* 1. Planning (PL)

### PL-1 Security Planning Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:

A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

Procedures to facilitate the implementation of the security planning policy and associated security planning controls; and

Reviews and updates the current:

Security planning policy [FedRAMP Assignment: at least every three (3) years]; and

* 1. Security planning procedures [FedRAMP Assignment: at least annually].

| PL-1 | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Trust Program Manager | |
| Parameter PL-01(a)(1):  Service Engineer Operations, Program Manager, Developer, Tester, Office 365 Trust Program Manager, Office 365 Security Manager, BCM | |
| Parameter PL-01(a)(2):  Service Engineer Operations, Program Manager, Developer, Tester, Office 365 Trust Program Manager, Office 365 Security Manager, BCM | |
| Parameter PL-01(b)(1):  annually | |
| Parameter PL-01(b)(2):  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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| PL-1 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Part 1:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Information Security Policy provides the overarching security guidance for Office 365 MT. This document addresses the purpose, scope, roles, responsibilities, compliance requirements, and required coordination among the various Microsoft organizations providing some level of support for the security of Office 365 MT. Policies are distributed to roles providing support for security planning via SharePoint.  **Part 2:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Standards and procedures to facilitate execution of these policies are documented in the Active Framework Controls, Office 365 Standard Operating Procedures (SOPs), and service team-specific SOPs. These standards and procedures act as adjuncts to the security policy and provide implementation level requirements and details to carry out specific operational tasks. A detailed mapping of Office 365 Standards and Procedures to each control is available. Office 365 SOPs are distributed to roles providing support for security via SharePoint. |
| Part b | **Part 1:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Information Security Policy is reviewed and updated annually.  **Part 2:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Standard Operating Procedures (SOPs) are reviewed and updated annually. |

### PL-2 System Security Plan (L) (M) (H)

The organization:

1. Develops a security plan for the information system that:
   1. Is consistent with the organization’s enterprise architecture;
   2. Explicitly defines the authorization boundary for the system;
   3. Describes the operational context of the information system in terms of missions and business processes;
   4. Provides the security categorization of the information system including supporting rationale;
   5. Describes the operational environment for the information system and relationships with or connections to other information;
   6. Provides an overview of the security requirements for the system;
   7. Identifies any relevant overlays, if applicable;
   8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and
   9. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation;
2. Distributes copies of the security plan and communicates subsequent changes to the plan to [Assignment: organization-defined personnel or roles];
3. Reviews the security plan for the information system [FedRAMP Assignment: at least annually];
4. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and
5. Protects the security plan from unauthorized disclosure and modification.

| PL-2 | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Trust Program Manager | |
| Parameter PL-02(b):  Office 365 Trust Program Manager, Program Manager | |
| Parameter PL-02(c):  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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| PL-2 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Part 1,2,3,4,5,6,7,8,9:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 MT System Security Plan provides an overview of the security requirements for Office 365 MT and the systems and applications within. Additionally, it contains a description of the security controls that are in place to meet those requirements.  The System Security Plan is created in accordance with NIST Special Publication 800-18, Revision 1, which contains guidance on security planning. This includes accurately defining the Office 365 MT accreditation boundary, as well as describing the operational environment, the security controls that are applicable to the system, and the system interconnections.  The System Security Plan documents the security categorization of the system based on the typical information being stored, processed or transmitted in Office 365 MT.  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). |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The System Security Plan is posted on the internal Office 365 MT SharePoint and distributed to the Office 365 Trust Program Manager and service team Program Managers. |
| Part c | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 Trust works with the System Owners to review and update the System Security Plan on an annual basis or when there is a major change to the system. |
| Part d | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Updates are made to the Office 365 MT System Security Plan as changes are made to the system or the operating environment to ensure the plan represents an accurate depiction of the Office 365 MT security posture. |
| Part e | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The System Security Plan is posted on the internal Office 365 MT SharePoint and protected using SharePoint Online’s built-in confidentiality and integrity protection mechanisms. |

#### PL-2 (3) Control Enhancement (M) (H)

The organization plans and coordinates security-related activities affecting the information system with [Assignment: organization-defined individuals or groups] before conducting such activities in order to reduce the impact on other organizational entities.

| PL-02(3) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Trust Program Manager | |
| Parameter PL-02(3):  Service Engineer Operations personnel, 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| PL-02(3) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 establishes coordination requirements among organizations in order to determine if security-related activities are going to affect Office 365 MT.  Office 365 MT plans and coordinates security-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-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 understanding what is required to support such activities. If activities involve Azure, they are included in planning as well. |

### PL-4 Rules of Behavior (L) (M)

The organization:

1. Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage;

Receives a signed 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 information system;

1. Reviews and updates the rules of behavior [FedRAMP Assignment: at least every three (3) years]; and
2. Requires individuals who have signed a previous version of the rules of behavior to read and resign when the rules of behavior are revised/updated.

| PL-4 | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Trust Program Manager | |
| Parameter PL-04(c):  every 3 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| PL-4 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility:**  Government customers are responsible for ensuring that government customer users acknowledge and sign the government customer’s rules of behavior for Office 365 MT. Non-government customers may not be required to have rules of behavior.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 MT Rules of Behavior describes Microsoft user responsibilities and establishes expected behavior when using Office 365 MT and other Microsoft systems. All Microsoft users, including employees, vendors, and contractors are required to follow the rules of behavior, which are outlined in the Office 365 MT Rules of Behavior. The agreements are put in place to protect trade secrets, sensitive, or business confidential information and assets.  The Non-Disclosure Agreement (NDA), Employee Handbook, and Office 365 Information Security Policy include statements regarding information and asset protection responsibilities. They also describe the penalties for the violation of these responsibilities.  Office 365 MT service team users are provided with all of these documents as part of annual security awareness training. Completion of the training constitutes employee acknowledgement and understanding of these documents. Additionally, the training ends with a test to verify the user’s understanding; passing the test is required and results are tracked by Office 365. |
| Part b | **Customer Responsibility:**  Government customers are responsible for ensuring that government customer users acknowledge and sign the government customer’s rules of behavior for Office 365 MT. Non-government customers may not be required to have rules of behavior.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  All full-time employees and contingent staff must sign appropriate agreements to acknowledge the terms and conditions of their employment and their understanding and acceptance of the Microsoft corporate employment policies. All Office 365 MT staff are required to sign confidentiality and non-disclosure agreements (NDA), as well as the Microsoft Employee Handbook, at the time of hire as a condition for employment.  A signed confirmation from Microsoft users indicating understanding and agreement of the NDA is required of all staff upon hire to Microsoft.  Office 365 MT service team users are provided with all of these documents as part of annual security awareness training. Completion of the training constitutes employee acknowledgement and understanding of these documents. Additionally, the training ends with a test to verify the user’s understanding; passing the test is required and results are tracked by Office 365. |
| Part c | **Customer Responsibility:**  Government customers are responsible for reviewing and updating their rules of behavior at least every three years.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Microsoft and Office 365 MT review and update the Employee Handbook, the Non-Disclosure Agreement, and Office 365 Information Security Policy, and the Office 365 MT Rules of Behavior at least every three years. |
| Part d | **Customer Responsibility:**  Government customers are responsible for requiring individuals to read and re-sign the rules of behavior when the rules of behavior are revised or updated.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  After revisions, the revised document is included in annual security awareness training. |

#### PL-4 (1) Control Enhancement (M) (H)

The organization includes in the rules of behavior, explicit restrictions on the use of social media/networking sites and posting organizational information on public websites.

| PL-04(1) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Trust Program Manager | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| PL-04(1) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The security awareness training includes explicit restrictions on the use of social media/networking sites and posting organizational information on public websites. |

### PL-8 Information Security Architecture (M) (H)

The organization:

1. Develops an information security architecture for the information system that:

Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information;

Describes how the information security architecture is integrated into and supports the enterprise architecture; and

Describes any information security assumptions about, and dependencies on, external services;

1. Reviews and updates the information security architecture [FedRAMP Assignment: at least annually or when a significant change occurs] to reflect updates in the enterprise architecture; and

PL-8 (b) Additional FedRAMP Requirements and Guidance:

Guidance: Significant change is defined in NIST Special Publication 800-37 Revision 1, Appendix F, on Page F-7.

1. Ensures that planned information security architecture changes are reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurements/acquisitions.

| PL-8 | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Trust Program Manager | |
| Parameter PL-08(b):  annually or when required by changes to the organizational or 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| PL-8 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Part 1,2,3,4:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT develops and documents the security architecture which describes:  1. 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 Office 365 MT  2. The integration of Office 365 MT architecture into Azure architecture  3. Assumptions about and dependencies on external services. |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT reviews and updates the information security architecture annually and when significant changes are made to Microsoft Azure architecture. |
| Part c | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT updates this System Security Plan and all Office 365 MT procurement/acquisition procedures whenever the information security architecture changes. |

* 1. Personnel Security (PS)

### PS-1 Personnel Security Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls; and
2. Reviews and updates the current:
   1. Personnel security policy [FedRAMP Assignment: at least every three (3) years]; and
   2. Personnel security procedures [FedRAMP Assignment: at least annually].

| PS-1 | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Trust Program Manager | |
| Parameter PS-01(a)(1):  Service Engineer Operations, Program Manager, Developer, Tester, Office 365 Trust Program Manager, Office 365 Security Manager, BCM | |
| Parameter PS-01(a)(2):  Service Engineer Operations, Program Manager, Developer, Tester, Office 365 Trust Program Manager, Office 365 Security Manager, BCM | |
| Parameter PS-01(b)(1):  annually | |
| Parameter PS-01(b)(2):  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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| PS-1 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Part 1:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Information Security Policy provides the overarching security guidance for Office 365 MT. This document addresses the purpose, scope, roles, responsibilities, compliance requirements, and required coordination among the various Microsoft organizations providing some level of support for the security of Office 365 MT. This policy is distributed to roles providing support for personnel security via SharePoint.  **Part 2:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Information Security Policy contains policies that must be met in the delivery and operation of Office 365 MT. Standards and Procedures to facilitate execution of these policies are documented in the Active Framework Controls, Office 365 Standard Operating Procedures (SOPs), and service team-specific SOPs. These standards and procedures act as adjuncts to the security policy and provide implementation level requirements and details to carry out specific operational tasks. A detailed mapping of Office 365 Standards and Procedures to each control is available for review. Office 365 SOPs are distributed to roles providing support for personnel security via SharePoint. |
| Part b | **Part 1:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Information Security Policy is reviewed and updated annually by the Office 365 Trust team.  **Part 2:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 SOPs are reviewed and updated annually by the service teams and by Office 365 Trust. |

### PS-2 Position Categorization (L) (M)

The organization:

1. Assigns a risk designation to all positions;
2. Establishes screening criteria for individuals filling those positions; and
3. Reviews and revises position risk designations [FedRAMP Assignment: at least every three (3) years].

| PS-2 | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Trust Program Manager | |
| Parameter PS-02(c):  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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| PS-2 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility:**  Government customers are responsible for assigning risk designations to all positions of customer personnel that are using Office 365 MT that are consistent with the customer’s internal policies and procedures. Microsoft does not assign risk designations to positions of customer personnel.  Non-government customers should adhere to their respective regulatory and internal policies, but they may not be required to assign risk designations for personnel. Microsoft does not assign risk designations to positions of customer personnel.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT ensures that service team personnel, including third-party personnel, with access to Office 365 MT have risk designations in place based on role assignments. All Office 365 MT roles with access to customer content receive the "Cloud" risk designation for personnel security. Office 365 MT roles with access to Office 365 MT additionally have the risk designation "MT", as do WAC roles with access to customer content. |
| Part b | **Customer Responsibility:**  Government customers are responsible for establishing screening criteria that are consistent with their internal policies and procedures for personnel using Office 365 MT. Microsoft does not establish screening criteria for individuals hired by customers.  Non-government customers should adhere to their respective regulatory and internal policies, but they may not be required to establish personnel screening criteria. Microsoft does not establish screening criteria for individuals hired by customers.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT, in coordination with Microsoft HR, has established screening criteria for Office 365 MT service team personnel by reviewing positions for risk as well as considering customer expectations. Screening criteria are documented at the following link and summarized below:  http://hrweb/career/jobs/policies/Pages/BackgroundSpecializedScreensUS.aspx  Roles with the “Cloud” risk designation are screened against the following:  • Social Security Number Search  • Criminal History Check  • Office of Foreign Assets Control List  • Bureau of Industry and Security List  • Office of Defense Trade Controls Debarred Persons  Roles with the “MT” risk designation are screened against the “Cloud” requirements, and the following additional criteria:  • United States Citizenship verification  • FBI fingerprinting  • CJIS  • GSA PTP-M (pending agency sponsor)? |
| Part c | **Customer Responsibility:**  Government customers are responsible for reviewing and revising position risk designations for personnel using Office 365 MT in a manner consistent with its internal policies and procedures. Microsoft does not review or revise position risk designations for customer personnel.  Non-government customers should adhere to their respective regulatory and internal policies, but they may not be required to assign, review, or revise risk designations for personnel. Microsoft does not review or revise position risk designations for customer personnel.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Microsoft Global Security is responsible for reviewing the risk designations and screening criteria listed in part b of this control at least annually. This review is conducted in a meeting with Office 365 management and Microsoft Corporate, External Legal Affairs (CELA). |

### PS-3 Personnel Screening (L) (M) (H)

The organization:

1. Screens individuals prior to authorizing access to the information system; and
2. Rescreens individuals according to [FedRAMP Assignment: 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 Role: Office 365 Trust Program Manager | |
| Parameter PS-03(b):  Microsoft internal requirements (background check redone every two years) or United States government requirements (security clearances renewed as appropriate) | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| PS-3 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility:**  Government customers are responsible for determining screening requirements and implementing those requirements for their own personnel before they grant them access to the system.  Non-government customers should adhere to their respective regulatory and internal policies, but they may not be required to perform personnel screening.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Microsoft screens personnel prior to providing access to customer content. "Cloud" background checks are required to be completed prior to creating an Office 365 MT service team account with access to this data.  The "Cloud" background check includes checking:  • Social Security Number Search  • Criminal History Check  • Office of Foreign Assets Control List  • Bureau of Industry and Security List  • Office of Defense Trade Controls Debarred Persons  Personnel requesting additional access to a MT role type are required to undergo additional screening, including:  • United States Citizenship verification  • FBI fingerprinting  • CJIS  Enforcing screening requirements at the time of account creation and permission assignment ensures that personnel will not be inadvertently granted access prior to successful screening. |
| Part b | **Customer Responsibility:**  Government customers are responsible for determining rescreening requirements and implementing those requirements for their own personnel.  Non-government customers should adhere to their respective regulatory and internal policies, but they may not be required to rescreen personnel on any recurring cadence.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT personnel with "Cloud" and "MT" designations are rescreened every two years. Access to the system is revoked for personnel who do not pass rescreening. |

#### PS-3 (3) Control Enhancement (M) (H)

The organization ensures that individuals accessing an information system processing, storing, or transmitting information requiring special protection:

1. Have valid access authorizations that are demonstrated by assigned official government duties; and
2. Satisfy [FedRAMP Assignment: personnel screening criteria – as required by specific information].

| PS-3 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Trust Program Manager | |
| Parameter PS-03(3)(b):  defined 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| PS-3 (3) - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility:**  Government customers are responsible for ensuring that their users accessing Office 365 MT have valid access authorizations that are demonstrated by their assigned official government duties.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT personnel are required to satisfy “Cloud” or “MT” screening as appropriate. |
| Part b | **Customer Responsibility:**  Government customers are also responsible for ensuring that their users accessing Office 365 MT satisfy additional personnel screening criteria as defined by the particular customer.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT personnel are required to satisfy “Cloud” or “MT” screening as appropriate. |

### PS-4 Personnel Termination (L) (M)

The organization, upon termination of individual employment:

1. Disables information system access within [FedRAMP Assignment: same day];
2. Terminates/revokes any authenticators/credentials associated with the individual;
3. Conducts exit interviews that include a discussion of [Assignment: organization-defined information security topics];
4. Retrieves all security-related organizational information system-related property;
5. Retains access to organizational information and information systems formerly controlled by terminated individual; and
6. Notifies [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period].

| PS-4 | Control Summary Information |
| --- | --- |
| Responsible Role: Human Resources, Program Manager | |
| Parameter PS-04(a):  24 hours | |
| Parameter PS-04(c):  non-disclosure agreements | |
| Parameter PS-04(f):  1. Human Resources & personnel's manager; 2. 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| PS-4 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility:**  Office 365 MT government and non-government customers are responsible for managing information system access terminations for their organizational users consistent with their internal policies and procedures.  Government and non-government customers, using ADFS, manage user accounts in their own customer-owned and controlled Active Directory (AD) forests. These customers may disable or delete terminated users in their internal AD infrastructure. When customers disable or delete users in their AD forests, access to Office 365 MT is immediately revoked for the disabled or terminated user. For additional more information on managing user accounts in Active Directory, see TechNet article #754661: http://technet.microsoft.com/en-us/library/cc754661.aspx  Non-government customers not using ADFS will manage accounts in AAD via the SUE portal. Non-government customers who manage accounts in AAD via SUE should disable/delete the user in the SUE portal; updating permissions in the portal will immediately revoke access for the terminated user. For additional more information on managing user accounts via the SUE portal, see TechNet article “office 365 user account management”: http://technet.microsoft.com/en-us/library/office-365-user-account-management.aspx  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Microsoft Human Resources is responsible for the personnel termination process. When an employee is terminated from Microsoft, the employee is removed from the Human Resources Information System (HRIS) via a termination transaction approved by the Human Resources Assistant (HRA) or Business Administrator. Once the transaction has been keyed in and approved, Microsoft Accounts and Security teams are notified and access to Office 365 MT is revoked.  Service team Active Directory domain accounts are tied to Microsoft account management tools for automated account management. Microsoft account management tools synchronize with the HRIS. When a service team user's employment is marked as terminated in HRIS, this information propagates to the Microsoft account management tools, which then automatically remove the service team domain account.  For involuntary terminations, an urgent request for access termination is submitted via email from HR and all access is immediately disabled by service team administrators. |
| Part b | **Customer Responsibility:**  Office 365 MT customers are responsible for revoking credentials of organizational users upon termination, consistent with their internal policies and guidelines.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  When a user's employment is terminated with Microsoft, the employee is removed from the Human Resources Information System (HRIS) via a termination transaction approved by the Human Resources Assistant (HRA) or Business Administrator. Microsoft account management tools synchronize with the HRIS. When a service team user's employment is marked as terminated in HRIS, this information propagates to Microsoft account management tools, which then automatically remove the service team domain account.  Human Resources Assistants or the employee's manager collect Microsoft badges at the time of the exit interview or termination. |
| Part c | **Customer Responsibility:**  Office 365 MT customers are responsible for conducting exit interviews for their terminated organizational users consistent with their internal policies and guidelines.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Human resource assistants or the employee’s manager conduct exit interviews on or before the employee's last day at Microsoft for employees resigning voluntarily. Topics covered in the exit interviews include review of non-disclosure agreements. Exit interviews may not be conducted in the event of a non-voluntary termination. |
| Part d | **Customer Responsibility:**  Office 365 MT customers are responsible for retrieving all security-related, organizational information system-related property for their terminated organizational users consistent with their internal policies and guidelines.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Human resource assistants or the terminated employee's manager collect Microsoft badges at the time of the exit interview or termination. Business Administrators and/or managers of the terminated employee collect hardware assets at the time of termination. These processes ensure that Microsoft collects all security-related, organizational information system-related property prior to the terminated user’s departure. |
| Part e | **Customer Responsibility:**  Office 365 MT customers are responsible for retaining access to organizational information and information systems formerly controlled by terminated individual for their terminated organizational users consistent with their internal policies and guidelines.  When an Office 365 MT account is deleted, it becomes inactive. For approximately 30 days after having deleted it, customers can restore the account. For more information about deleting and restoring accounts, see TechNet article “office 365 user account management”: http://technet.microsoft.com/en-us/library/office-365-user-account-management.aspx  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  When an employee is terminated from Microsoft, the employee is removed from the Human Resources Information System (HRIS) via a termination transaction and approved by the Human Resources Assistant (HRA) or Business Administrator. Once the request is submitted and approved, Microsoft Accounts and Security teams are notified and access to the information system and buildings is shut off, via the HRIS termination transaction process and/or urgent terminations email template. For involuntary terminations, an urgent request for access termination is submitted via email from HR and all access is immediately disabled. All customer content is retained in the production environment and accessible by authorized personnel for Office 365 MT. This ensures that Microsoft retains access to organizational information and information systems formerly controlled by terminated employees. |
| Part f | **Customer Responsibility:**  Office 365 MT customers are responsible for notifying the proper personnel upon termination of their organizational users consistent with their internal policies and guidelines.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  When an employee is terminated from Microsoft, the employee’s manager is notified within 24 hours. |

### PS-5 Personnel Transfer (L) (M)

The organization:

1. Reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization;
2. Initiates [Assignment: organization-defined transfer or reassignment actions] within [Assignment: organization-defined time period following the formal transfer action];
3. Modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and
4. Notifies [Assignment: organization-defined personnel or roles] within [FedRAMP Assignment: within five days of the formal transfer action (DoD 24 hours)].

| PS-5 | Control Summary Information |
| --- | --- |
| Responsible Role: Program Manager | |
| Parameter PS-05(b):  1. actions to ensure all system accesses no longer required are removed; 2. 5 days | |
| Parameter PS-05(d):  1. transferring personnel's manager; 2. 5 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| PS-5 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility:**  Government customers are responsible for reviewing logical access authorizations to Office 365 MT for their own personnel prior to reassigning or transferring to another position within their organization and granting access to Office 365 MT.  Non-government customers should adhere to their respective regulatory and internal personnel transfer policies and review of logical and physical access authorizations. Non-government customers not using ADFS may mange accounts via the Suite User Experience (SUE) portal. Customers are responsible for logging into the portal and reviewing the Office 365 MT accounts of their users compliant with their organizational policies. Disabling or removing users in the SUE portal revokes access to Office 365 MT for the affected users. For additional more information on managing user accounts via the SUE portal, see TechNet article “Office 365 user account management”: http://technet.microsoft.com/en-us/library/office-365-user-account-management.aspx  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  When an employee is reassigned or transfers to a position within a different cost center, a Human Resources Information System (HRIS) transfer transaction is keyed into the HRIS system. This transfer transaction is sent to Microsoft account management tools, which notify the role owner of any Office 365 MT roles assigned to the employee. The role owner is then responsible for determining if the employee still requires their current access and responding accordingly.  Office 365 MT personnel do not have physical access to the information system. |
| Part b | **Customer Responsibility:**  Government customers are responsible for initiating transfer or reassignment actions pertaining to Office 365 MT within a specified timeframe after their own personnel have been formally transferred.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Microsoft Human Resources is responsible for ensuring personnel transfer is handled within 5 days of initiation for personnel who are reassigned or transferred to other positions within the organization. Microsoft defines the transfer or reassignment actions to implement through the use of the Human Resources Information System (HRIS), which is managed by Microsoft Human Resources.  For personnel transfers with security implications, system accesses and security group memberships are re-evaluated to reflect the user’s new role and responsibilities immediately. |
| Part c | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  See PS-5(a). |
| Part d | **Customer Responsibility:**  Government customers are responsible for notifying the proper personnel within a specified timeframe after their own personnel have been formally transferred.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Microsoft Human Resources is responsible for ensuring personnel transfer is handled within 5 days of initiation for personnel who are reassigned or transferred to other positions within the organization. Microsoft defines the transfer or reassignment actions to implement through the use of the Human Resources Information System (HRIS), which is managed by Microsoft Human Resources. When an employee transfers to a position within a different cost center, an HRIS transfer transaction is submitted to HRIS system. This transfer is transmitted to Microsoft account management tools, which notify the role owner of any Office 365 MT roles assigned to the employee. |

### PS-6 Access Agreements (L) (M)

The organization:

1. Develops and documents access agreements for organizational information systems;
2. Reviews and updates the access agreements [FedRAMP Assignment: at least annually]; and
3. Ensures that individuals requiring access to organizational information and information systems:
   1. Sign appropriate access agreements prior to being granted access; and
   2. Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or [FedRAMP Assignment: at least annually].

| PS-6 | Control Summary Information |
| --- | --- |
| Responsible Role: Program Manager | |
| Parameter PS-06(b):  at least annually | |
| Parameter PS-06(c)(2):  when there is a change to the user's level of access, 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| PS-6 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility:**  Government customers are responsible for developing and documenting access agreements for organizational information systems.  Non-government customers should adhere to their respective regulatory and internal policies, but they may not be required to ensure that they have developed and documented access agreements for organizational information systems.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Microsoft has developed and documented confidentiality and non-disclosure agreements, as well as the Microsoft Employee Handbook access agreements, which Office 365 MT staff are required to sign as a condition for employment and access to Office 365 MT. Additionally, Microsoft has developed the Office 365 MT Rules of Behavior, which all users are required to follow when using Office 365 MT. Microsoft has also developed the Master Supplier Services Agreement (MSSA) that vendors and contractors are required to sign to ensure compliance with Microsoft policies on required engagements. |
| Part b | **Customer Responsibility:**  Government customers are responsible for reviewing and updating the customer access agreements at least annually.  Non-government customers should adhere to their respective regulatory and internal policies, but they may not be required to use, review, and update access agreements.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Employee Handbook, confidentiality and non-disclosure agreements, Office 365 MT Rules of Behavior, and the Master Supplier Services Agreement (MSSA) are reviewed and updated annually to reflect changes in the Microsoft environment. As described in PL-4, Office 365 MT service team users are provided with all of these documents as part of annual security awareness training. Submission of training completion constitutes agreement that the user understands these documents. |
| Part c | **Customer Responsibility:**  Government customers are responsible for ensuring that users with access to Office 365 MT sign appropriate customer access agreements prior to being granted access, and that employees renew these agreements on an organization-defined frequency.  Non-government customers should adhere to their respective regulatory and internal policies, but they may not be required to ensure that individuals sign access agreements prior to being granted access or that employees renew these agreements.  **Part 1:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  All Office 365 MT staff are required to sign confidentiality and non-disclosure agreements, as well as the Microsoft Employee Handbook access agreements, at the time of hire as a condition for employment and access to Office 365 MT. Additionally, the Office 365 MT Rules of Behavior describes Microsoft user responsibilities and establishes expected behavior when using Office 365 MT. All users, including employees, vendors, and contractors are required to follow the rules of behavior outlined in the Office 365 MT Rules of Behavior. Vendors and contractors are required to have a signed Master Supplier Services Agreement (MSSA) to ensure compliance with Microsoft policies on required engagements.  The Non-Disclosure Agreement (NDA), Employee Handbook, and the Office 365 MT Rules of Behavior include statements regarding information and asset protection responsibilities. They also describe the penalties for the violation of these responsibilities. A signed confirmation from users indicating understanding and agreement of the NDA is required of all users prior to gaining access to the Microsoft network. The NDA is tracked and enforced by HR while the Service Team PMs are responsible for submitting the agreements after they have been signed.  **Part 2:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT administrators are privileged users within their respective environments and their access level does not change for their role. Therefore, it is not necessary to re-sign original access agreements to maintain access, as access levels do not change.  Office 365 MT administrators are required to complete annual security awareness training, which includes review of system access agreements. Completion of the training constitutes employee acknowledgement and understanding of these documents, and is used in place of a signature.  Master Supplier Services Agreements (MSSA)’s are not annually renewed. Instead statements of work (SOWs) are updated at least annually, and SOWs are attached to the Master Supplier Services Agreement (MSSA) template which contains the NDA. By updating SOWs at least annually, external vendors inherently re-agree to their current NDAs.  Microsoft has documented this decision in the Decision Log “FedRAMP PS-6: Access Agreements Are Not Annually Renewed”. |

### PS-7 Third-Party Personnel Security (L) (M)

The organization:

1. Establishes personnel security requirements including security roles and responsibilities for third-party providers;
2. Requires third-party providers to comply with personnel security policies and procedures established by the organization;
3. Documents personnel security requirements;
4. Requires third-party providers to notify [Assignment: organization-defined personnel or roles] of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within [FedRAMP Assignment: same day]; and
5. Monitors provider compliance.

| PS-7 | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Trust Program Manager, Program Manager | |
| Parameter PS-07(d):  1. business relationship owner; 2. 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| PS-7 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility:**  Government customers are responsible for establishing personnel security requirements, including security roles and responsibilities, for third-party providers with access to Office 365 MT.  Non-government customers should adhere to their respective regulatory and internal policies, but they may not be required to establish personnel screening requirements for third-party providers with access to Office 365 MT.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  In all contracts, Microsoft establishes screening requirements for third-party providers to ensure that third-party providers meet or exceed the personnel security requirements mandated by Microsoft. Any third-party personnel with access to Office 365 MT must pass the same personnel screening process (described in PS-3) for the requirements established for the risk categorization of their role (described in PS-2). |
| Part b | **Customer Responsibility:**  Government customers are responsible for requiring compliance with security requirements for third-party personnel with access to Office 365.  Non-government customers should adhere to their respective regulatory and internal policies, but they may not be required to perform personnel screening.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT requires vendors and contractors to have a signed Master Supplier Services Agreement (MSSA) to ensure compliance with Microsoft policies and procedures, including personnel security policies and procedures, on required engagements. |
| Part c | **Customer Responsibility:**  Government customers are responsible for documenting third-party personnel security requirements for third-party personnel with access to Office 365.  Non-government customers should adhere to their respective regulatory and internal policies, but they may not be required to perform personnel screening.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT documents third-party security requirements via the Microsoft background screening requirements. Specific personnel screening requirements for third-party roles with access to Office 365 MT are identical to those for Microsoft personnel. |
| Part d | **Customer Responsibility:**  Government customers are responsible for notifying the proper personnel upon transfer or termination of third-party personnel with access to Office 365.  Non-government customers should adhere to their respective regulatory and internal policies, but they may not be required to notify personnel upon transfer or termination actions.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT requires vendors and contractors to comply with Microsoft policies and procedures, including third-party security requirements. Third-party agreement is documented in the Master Supplier Services Agreement (MSSA). Specific notification requirements for transfers and terminations of third-party personnel with access to Office 365 MT are identical to those for Microsoft personnel. |
| Part e | **Customer Responsibility:**  Government customers are responsible for monitoring provider compliance with third-party personnel security requirements for third-party personnel with access to Office 365.  Non-government customers should adhere to their respective regulatory and internal policies, but they may not be required to monitor provider compliance with third-party personnel security requirements for third-party personnel with access to Office 365.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Any third-party personnel with access to Office 365 MT must pass the same personnel screening process (described in PS-3) for the requirements established for the risk categorization of their role (described in PS-2). Office 365 MT 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.  Office 365 MT personnel who have access to customer content are rescreened every two years. |

### PS-8 Personnel Sanctions (L) (M)

The organization:

1. Employs a formal sanctions process for personnel failing to comply with established information security policies and procedures; and
2. Notifies [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period] when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

| PS-8 | Control Summary Information |
| --- | --- |
| Responsible Role: Human Resources, Office 365 Trust Program Manager, Program Manager | |
| Parameter PS-08(b):  1. HR and the employee's manager; 2. 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| PS-8 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility:**  Government customers are responsible for determining, based on applicable laws and regulatory policies, appropriate sanctions against personnel who have committed security violations pertaining to Office 365 MT.  Non-government customers should adhere to applicable regulatory and internal policies when imposing sanctions on personnel.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Microsoft’s formal sanctions process is defined in the Microsoft Employee Handbook. Corporate Security is responsible for ensuring that the sanctions process is conducted properly. All potential security breaches involving Office 365 MT employees or third-party personnel will be immediately reported to Human Resources, the Corporate, External, & Legal Affairs (CELA) and the transgressing Microsoft employee's manager.  All violations prompt an investigation of the incident, and the Microsoft employee will be subject to appropriate disciplinary action, up to and including termination. If the investigation finds that the Microsoft employee committed a breach of security, Human Resources will be informed and take responsibility for coordinating the disciplinary response. Third-party personnel suspected of committing violations will be subject to formal investigation and action appropriate to the associated contract, which may include termination of said contract.  In some cases, a violation of Microsoft’s security policies may also violate an international, federal, state, or local law, which may subject the individual to civil and/or criminal liability. |
| Part b | **Customer Responsibility:**  Government customers are responsible for notifying the proper personnel once sanctions are taken against personnel who have committed security violations pertaining to Office 365 MT.  Non-government customers should adhere to applicable regulatory and internal policies when imposing sanctions on personnel.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT notifies Human Resources and the transgressing Microsoft employee's manager within 24 hours when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction. |

* 1. Risk Assessment (RA)

### RA-1 Risk Assessment Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls; and
2. Reviews and updates the current:
   1. Risk assessment policy [FedRAMP Assignment: at least every three (3) years]; and
   2. Risk assessment procedures [FedRAMP Assignment: at least annually].

| RA-1 | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Trust Program Manager | |
| Parameter RA-01(a)(1):  Service Engineer Operations, Program Manager, Developer, Tester, Office 365 Trust Program Manager, Office 365 Security Manager, BCM | |
| Parameter RA-01(a)(2):  Service Engineer Operations, Program Manager, Developer, Tester, Office 365 Trust Program Manager, Office 365 Security Manager, BCM | |
| Parameter RA-01(b)(1):  annually | |
| Parameter RA-01(b)(2):  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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| RA-1 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Part 1:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Information Security Policy provides the overarching security guidance for Office 365 MT. This document addresses the purpose, scope, roles, responsibilities, compliance requirements, and required coordination among the various Microsoft organizations providing some level of support for the security of Office 365 MT. The policy is distributed to roles providing support for risk assessments via SharePoint.  **Part 2:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Information Security Policy contains policies that must be met in the delivery and operation of Office 365 MT. Standards and procedures to facilitate execution of these policies are documented in the Active Framework Controls, Office 365 Standard Operating Procedures (SOPs), and service team-specific SOPs. These standards and procedures act as adjuncts to the security policy and provide implementation level requirements and details to carry out specific operational tasks. A detailed mapping of Office 365 Standards and Procedures to each control is available for review. Office 365 SOPs are distributed to roles providing support for risk assessment via SharePoint. |
| Part b | **Part 1:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Information Security Policy is reviewed and updated annually by the Office 365 Trust team.  **Part 2:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 SOPs are reviewed and updated annually by the service teams and by Office 365 Trust. |

### RA-2 Security Categorization (L) (M) (H)

The organization:

1. Categorizes information and the information system in accordance with applicable Federal Laws, Executive Orders, directives, policies, regulations, standards, and guidance;
2. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and
3. Ensures the security categorization decision is reviewed and approved by the AO or authorizing official designated representative.

| RA-2 | Control Summary Information |
| --- | --- |
| Responsible Role: Customer Administrator, Office 365 Trust Program Manager | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| RA-2 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility:**  Government customers are responsible for ensuring that no information with a security impact level greater than moderate is stored, processed, or transmitted via the services provided to them by Office 365 MT.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT has completed an Assessment and Authorization (A&A) package to be authorized to operate at FIPS 199 Moderate impact level. Based on FIPS 199 standards, Office 365 MT service teams identified a selection of information types based on system components within Office 365 MT core offerings.  Utilizing this selection, Office 365 MT categorized information types and evaluated the impact on the organization from compromise of confidentiality, loss of integrity or lack of availability (CIA).  Because Office 365 MT does not have control over the information customers store within the system, government customer agencies/departments must separately categorize their data in agreement with FIPS 199 and NIST 800-60 to ensure that the security category of information types collected, processed, or stored in Office 365 MT does not exceed Moderate impact for confidentiality, integrity, and/or availability. |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The security categorization for Office 365 MT has been conducted and is documented in detail in section 2.2 of this SSP. The overall security categorization has been assessed at the Moderate impact level for confidentiality, integrity, and availability as determined in accordance with FIPS 199 guidelines and the Office 365 MT FIPS 199 categorization. The security categorization process took into consideration supporting rationale for impact-level decisions and involved appropriate stakeholders and senior-level organizational officials (program management, system owner) to review and approve the final security categorization activity. |
| Part c | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Microsoft has provided the FIPS 199 Security categorization assessment in the Office 365 MT security authorization package for the review and approval of the JAB and subsequent customer agencies that may leverage the Office 365 MT Security Authorization Package. |

### RA-3 Risk Assessment (L) (M)

The organization:

1. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;
2. Documents risk assessment results in [Selection: security plan; risk assessment report; [FedRAMP Assignment: security assessment report]];
3. Reviews risk assessment results [FedRAMP Assignment: in accordance with OMB A-130 requirements or when a significant change occurs];
4. Disseminates risk assessment results to [Assignment: organization-defined personnel or roles]; and
5. Updates the risk assessment [FedRAMP Assignment: in accordance with OMB A-130 requirements or when a significant change occurs] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

RA-3 Additional FedRAMP Requirements and Guidance:

Guidance: Significant change is defined in NIST Special Publication 800-37 Revision 1, Appendix F

RA-3 (d) Requirement: Include the Authorizing Official; for JAB authorizations to include FedRAMP.

| RA-3 | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Trust Program Manager | |
| Parameter RA-03(b):  Risk Assessment Report | |
| Parameter RA-03(c):  annually or when a significant change occurs | |
| Parameter RA-03(d):  Office 365 Trust Program Manager | |
| Parameter RA-03(e):  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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| RA-3 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  As part of establishing an Information Security Management System ("ISMS") for Office 365 MT, a risk assessment methodology was developed to provide a structured approach to risk management and to prioritize and direct Office 365 MT Risk Management activities. This methodology has been designed in compliance with NIST SPs 800-30 and 800-37 and comprises the following four phases to accomplish a successful risk management process. Details of the methodology are available for 3PAO review in the document named Office 365 Risk Management SOP:  1. Identify – Threat, Vulnerability, and Risk identification provides the list of risks which exist in the environment and provides a basis for all other risk management activities  2. Assess – The risk assessment considers the potential impact of an information security risk to the business and its likelihood of occurrence; determine appropriate risk treatment plan to reduce risk to a desirable level  3. Report – Risk reports provide managers with the data they need to make effective business decisions and to comply with internal policies and industry regulations  4. Monitor – Risk groups perform testing and monitoring activities to evaluate whether processes, initiatives, functions, and/or activities are mitigating the risk as designed  The Risk Assessment Assess phase begins with identifying risks, establishing a risk level by determining the likelihood of occurrence and impact, and finally, identifying controls and safeguards that reduce the impact of the risk to an acceptable level. |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT documents risk assessment results in an annual risk assessment report. |
| Part c | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT business owners annually perform a business risk assessment using NIST SP 800-30 and 800-37 guidelines to ascertain the risk associated with operating Office 365 MT and to ensure financial and operational viability. The results of the risk assessment are documented in business and capital planning documentation.  Office 365 MT Trust annually reviews existing assessments and performs security assessments to understand the risk posture of the service and to ensure security standards compliance. The results of the security assessment are captured in a Risk Assessment Report. |
| Part d | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT submits risk assessment results to Office 365 MT management, including the Office 365 Trust Program Managers. |
| Part e | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 Trust ensures that a risk assessment is conducted at least annually, or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system. The assessments follow the process described in Part (a) of this control. |

### RA-5 Vulnerability Scanning (L) (M) (H)

The organization:

1. Scans for vulnerabilities in the information system and hosted applications [FedRAMP Assignment: monthly operating system/infrastructure; monthly web applications and databases] and when new vulnerabilities potentially affecting the system/applications are identified and reported;

RA-5 (a) Additional FedRAMP Requirements and Guidance:

Requirement: An accredited independent assessor scans operating systems/infrastructure, web applications, and databases once annually.

1. Employs vulnerability scanning tools and techniques that promote 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 and making transparent, checklists and test procedures; and
   3. Measuring vulnerability impact;
2. Analyzes vulnerability scan reports and results from security control assessments
3. Remediates legitimate vulnerabilities; [FedRAMP Assignment: high-risk vulnerabilities mitigated within thirty (30) days from date of discovery; moderate risk vulnerabilities mitigated within ninety (90) days from date of discovery], in accordance with an organizational assessment of risk; and
4. Shares information obtained from the vulnerability scanning process and security control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

RA-5 (e) Additional FedRAMP Requirements and Guidance:

Requirement: To include the Risk Executive; for JAB authorizations to include FedRAMP ISSOs.

| RA-5 | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager | |
| Parameter RA-05(a):  monthly | |
| Parameter RA-05(d):  in accordance with the Office 365 policy (high-risk vulnerabilities mitigated in 30 days; medium-risk vulnerabilities mitigated within 90 days) | |
| Parameter RA-05(e):  Office 365 Security Manager, Office 365 Trust Program Manager | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| RA-5 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Vulnerability scanning in the Office 365 MT environment is conducted by Office 365 Security using BeyondTrust. These scans include operating system, infrastructure, database and application scans.  Vulnerability scans are configured to run at least monthly and include all Office 365 MT systems. Scans are also run whenever new vulnerabilities potentially affecting Office 365 MT are discovered. During the annual 3PAO assessment, the scans will be supervised by the 3PAO but performed by Office 365 MT personnel. |
| Part b | **Part 1:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT uses the BeyondTrust scanning tool; this tool expresses vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and uses the Open Vulnerability Assessment Language (OVAL) to facilitate interoperability among tools. Office 365 Security also provides a reporting interface to allow authorized Office 365 MT personnel to see the details of vulnerabilities associated with the environment. The reporting interface provides high-level / technical reports (covering information such as servers, vulnerabilities, CVE IDs, breakdowns of vulnerable hosts, and remediation steps). The Office 365 MT service teams utilize the information on the reporting interface to ensure that servers are compliant with Office 365 MT vulnerability management standards.  **Part 2:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT uses the BeyondTrust scanning tool; this tool expresses vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and uses the Open Vulnerability Assessment Language (OVAL) to facilitate interoperability among tools. Office 365 Security also provides a reporting interface to allow authorized Office 365 MT personnel to see the details of vulnerabilities associated with the environment. The reporting interface provides high-level / technical reports (covering information such as servers, vulnerabilities, CVE IDs, breakdowns of vulnerable hosts, and remediation steps). The Office 365 MT service teams utilize the information on the reporting interface to ensure that servers are compliant with Office 365 MT vulnerability management standards.  **Part 3:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT uses the BeyondTrust scanning tool; this tool expresses vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and uses the Open Vulnerability Assessment Language (OVAL) to facilitate interoperability among tools. Office 365 Security also provides a reporting interface to allow authorized Office 365 MT personnel to see the details of vulnerabilities associated with the environment. The reporting interface provides high-level / technical reports (covering information such as servers, vulnerabilities, CVE IDs, breakdowns of vulnerable hosts, and remediation steps). The Office 365 MT service teams utilize the information on the reporting interface to ensure that servers are compliant with Office 365 MT vulnerability management standards. |
| Part c | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 Security analyzes vulnerability scan reports at least monthly to ensure security and patch compliance. Results from security control assessments are also incorporated into remediation activities in coordination with Office 365 Trust. |
| Part d | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  All vulnerabilities identified by the vulnerability scanning process are classified by risk. Vulnerability remediation is conducted in accordance with Office 365 MT policy. High-risk vulnerabilities are mitigated within 30 days. Medium-risk vulnerabilities are mitigated within 90 days.  Vulnerabilities are tracked through remediation by Office 365 MT service teams. In the event where patching during the timeframe is infeasible and on case-by-case basis, service groups may request exceptions. |
| Part e | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT Security provides a reporting interface to allow authorized Office 365 MT personnel to see the details of vulnerabilities associated with the environment. The reporting interface provides high-level / technical reports (covering information such as servers, vulnerabilities, CVE IDs, breakdowns of vulnerable hosts, and remediation steps, etc.). Vulnerability reporting to government customers is accomplished through continuous monitoring reporting processes. |

#### RA-5 (1) Control Enhancement (M) (H)

The organization employs vulnerability scanning tools that include the capability to readily update the list of information system vulnerabilities to be scanned.

| RA-05(1) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| RA-05(1) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Vulnerability scanning in the Office 365 MT environment is conducted using BeyondTrust. BeyondTrust uses the vulnerability information from industry sources to scan the Office 365 MT environment. BeyondTrust has the capability to download new vulnerability information. Scanning processes include a check to ensure that this update has occurred before each use. The scan executes regardless of update to ensure a daily scan is done. |

#### RA-5 (2) Control Enhancement (M) (H)

The organization updates the information system vulnerabilities scanned [Selection (one or more): [FedRAMP Assignment: prior to a new scan]].

| RA-05(2) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager | |
| Parameter RA-05(2):  prior to a new scan | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| RA-05(2) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Vulnerability scanning in the Office 365 MT environment is conducted using BeyondTrust. BeyondTrust uses the vulnerability information from industry sources to scan the Office 365 MT environment. BeyondTrust has the capability to download new vulnerability information. Scanning processes include a check to ensure that this update has occurred before each use. |

#### RA-5 (3) Control Enhancement (M) (H)

The organization employs vulnerability scanning procedures that can demonstrate the breadth and depth of coverage (i.e., information system components scanned and vulnerabilities checked).

| RA-05(3) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| RA-05(3) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  BeyondTrust is configured to produce reports each time it is used that includes detailed information on what information system components were scanned and which vulnerabilities were checked. Office 365 MT scanning processes include checks to make sure this information is correctly recorded for each scan. |

#### RA-5 (5) Control Enhancement (M) (H)

The organization includes privileged access authorization to [FedRAMP Assignment: operating systems, databases, web applications] for selected [FedRAMP Assignment: all scans].

| RA-05(5) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager | |
| Parameter RA-05(5):  1. information system components including operating systems, and web applications; 2. full, detailed vulnerability and patch 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| RA-05(5) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  BeyondTrust is configured with privileged access credentials for all system components and for all operating system and database scanning activities.  POA&M MT-0119 has been opened to track web application scanning is not performed on a monthly basis using privileged access authorizations. |

#### RA-5 (6) Control Enhancement (M) (H)

The organization employs automated mechanisms to compare the results of vulnerability scans over time to determine trends in information system vulnerabilities.

RA-5(6) Additional FedRAMP Requirements and Guidance:

Guidance: Include in Continuous Monitoring ISSO digest/report to JAB/AO.

| RA-05(6) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager, 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| RA-05(6) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 Security has automated reporting to compare scan results over time. These reports are available to authorized personnel on the Office 365 MT Patching and Vulnerability Compliance (PAVC) dashboard. |

#### RA-5 (8) Control Enhancement (L) (M) (H)

The organization reviews historic audit logs to determine if a vulnerability identified in the information system has been previously exploited.

RA-5(8) Additional FedRAMP Requirements and Guidance:

Requirement: This enhancement is required for all high vulnerability scan findings.

Guidance: While scanning tools may label findings as high or critical, the intent of the control is based around NIST's definition of high vulnerability.

| RA-05(8) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| RA-05(8) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 Security Incident Response (SIR) is responsible for reviewing newly identified high findings and determining if they could have possibly been exploited; this determination includes reviews of audit logs as determined necessary by Office 365 Security Operations. |

* 1. System and Services Acquisition (SA)

### SA-1 System and Services Acquisition Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls; and
2. Reviews and updates the current:
   1. System and services acquisition policy [FedRAMP Assignment: at least every three (3) years]; and
   2. System and services acquisition procedures [FedRAMP Assignment: at least annually].

| SA-1 | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Trust Program Manager | |
| Parameter SA-01(a)(1):  Service Engineer Operations, Program Manager, Developer, Tester, Office 365 Trust Program Manager, Office 365 Security Manager, BCM | |
| Parameter SA-01(a)(2):  Service Engineer Operations, Program Manager, Developer, Tester, Office 365 Trust Program Manager, Office 365 Security Manager, BCM | |
| Parameter SA-01(b)(1):  Annually | |
| Parameter SA-01(b)(2):  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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SA-1 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Part 1:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Information Security Policy defines Office 365 MT policies. This document addresses the purpose, scope, roles, responsibilities, compliance requirements, and required coordination among the various Microsoft organizations providing some level of support for the security of Office 365 MT. Policies are made available to roles providing support for system and services acquisition via SharePoint.  **Part 2:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Information Security Policy contains policies that must be met in the delivery and operation of Office 365 MT. Standards and procedures to facilitate execution of these policies are documented in the Active Framework Controls, Office 365 Standard Operating Procedures (SOPs), and service team-specific SOPs. These standards and procedures act as adjuncts to the security policy and provide implementation level requirements and details to carry out specific operational tasks. A detailed mapping of Office 365 Standards and Procedures to each control is available. Office 365 SOPs are distributed to roles supporting system and services acquisition via SharePoint. |
| Part b | **Part 1:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Information Security Policy is reviewed and updated annually by the Office 365 Trust team.  **Part 2:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Standard Operating Procedures (SOPs) are reviewed and updated annually by the service teams and by Office 365 Trust. |

### SA-2 Allocation of Resources (L) (M) (H)

The organization:

1. Determines information security requirements for the information system or information system service in mission/business process planning;
2. Determines, documents, and allocates the resources required to protect the information system or information system service as part of its capital planning and investment control process; and
3. Establishes a discrete line item for information security in organizational programming and budgeting documentation.

| SA-2 | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager, Office 365 Trust Program Manager | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SA-2 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT includes a determination of information security requirements in business process planning. The requirements phase mandates 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.  Office 365 MT includes a determination of security requirements at the onset of a project to allow for development teams to identify key objects and integrate security and privacy, which minimizes disruption to plans and schedules. |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT implements the allocation of resources control as part the requirements phase of life cycle support. This phase requires documenting and allocating resources required to protect Office 365 MT consistently with all compliance obligations. |
| Part c | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT and each service team undergo a yearly budgeting process, which includes a line item for information security along with future security projections. This helps manage resources needed for new and existing activities and ensures adequate allocation of resources to protect the information system. |

### SA-3 System Development Life Cycle (L) (M) (H)

The organization:

1. Manages the information system using [Assignment: organization-defined system development life cycle] that incorporates information security considerations;
2. Defines and documents information security roles and responsibilities throughout the system development life cycle;
3. Identifies individuals having information security roles and responsibilities; and
4. Integrates the organizational information security risk management process into system development life cycle activities.

| SA-3 | Control Summary Information |
| --- | --- |
| Responsible Role: Developer, Office 365 Trust Program Manager, Program Manager, Tester | |
| Parameter SA-03(a):  Microsoft's Secure 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SA-3 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT’s implementation of life cycle support is followed by all engineering and development projects. This is a software development model that includes specific security considerations. A security requirements analysis must be completed for all system development projects. This analysis document acts as a framework and includes the identification of possible risks to the finished development project as well as mitigation strategies which can be implemented and tested during the development phases. Critical security review and approval checkpoints are included.  All members of software development teams receive appropriate training to stay informed about security basics and recent trends in security and privacy. Individuals who develop software programs are required to attend at least one security training class each year. Security training helps ensure software is created with security and privacy in mind and also helps 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.  The process includes the following phases:  • Phase 1: Requirements - The requirements phase 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 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 will result 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. Initial testing of elements begins in this phase.  • 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 Response document 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.  After a software program 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 create a response plan that includes preparations for potential post-release issues.  Office 365 MT has implemented information validation through checking of data inputs as part of the process. Thorough code reviews and testing are completed during the Verification Phase prior to software 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.  This satisfies the life cycle support control through effective management of the risks associated with failing to implement a methodology that lacks information security considerations.  The following is a non-exhaustive list of software is used:  • Threat Modeling Tool: This tool helps developers analyze possible security issues.  • FxCop/OACR (Office Auto Code Review): FxCop/OACR assesses system software for consistency with code rules required. OACR also provides static code security analysis.  • BinScope: This tool analyzes software binaries for possible security issues.  • PREFast: This is a static code security analysis tool.  • FileFuzzer: This tool modifies system inputs dynamically to test for security weaknesses. |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC**  Office 365 MT defines security roles and responsibilities and identifies individuals with these roles and responsibilities. |
| Part c | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT defines security roles and responsibilities and identifies individuals with these roles and responsibilities. |
| Part d | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT integrates risk analysis, threat model analysis, and risk management practices. |

### SA-4 Acquisitions Process (L) (M) (H)

The organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs:

1. Security functional requirements;
2. Security strength requirements;
3. Security assurance requirements;
4. Security-related documentation requirements;
5. Requirements for protecting security-related documentation;
6. Description of the information system development environment and environment in which the system is intended to operate; and
7. Acceptance criteria.

Additional FedRAMP Requirements and Guidance:

Guidance: The use of Common Criteria (ISO/IEC 15408) evaluated products is strongly preferred.   
See http://www.niap-ccevs.org/vpl or http://www.commoncriteriaportal.org/products.html.

| SA-4 | Control Summary Information |
| --- | --- |
| Responsible Role: Customer Administrator, Office 365 Trust Program Manager | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SA-4 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility:**  Government customers must not use credit cards to purchase Office 365 MT. They must purchase Office 365 MT through a Purchasing Order.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT implements the acquisitions control through enforcement of the Office 365 Information Security Policy. The Office 365 Information Security Policy and associated standards (documented in the Active Framework Controls) 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 standards are addressed in the agreement, to provide a level of protection against identified risks equivalent to that provided by the Office 365 Information Security Policy.  It is the role of Corporate, External, & Legal Affairs (CELA) to approve all language included in system acquisition contracts pertaining to the security requirements. This includes the security functional requirements, security strength requirements, security assurance requirements, security-related documentation requirements, requirements for protecting security-related documentation, a description of the information system development environment and environment in which the system is intended to operate, and acceptance criteria, all of which are explained in detail in the documents mentioned above. Pre-existing third-party contracts are amended to include appropriate language upon renewal. This satisfies the acquisition control through effective management of the risks associated with failing to document security requirements in contracts. |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT implements the acquisitions control through enforcement of the Office 365 Information Security Policy. The Office 365 Information Security Policy and associated standards (documented in the Active Framework Controls) 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 standards are addressed in the agreement, to provide a level of protection against identified risks equivalent to that provided by the Office 365 Information Security Policy.  It is the role of Corporate, External, & Legal Affairs (CELA) to approve all language included in system acquisition contracts pertaining to the security requirements. This includes the security functional requirements, security strength requirements, security assurance requirements, security-related documentation requirements, requirements for protecting security-related documentation, a description of the information system development environment and environment in which the system is intended to operate, and acceptance criteria, all of which are explained in detail in the documents mentioned above. Pre-existing third-party contracts are amended to include appropriate language upon renewal. This satisfies the acquisition control through effective management of the risks associated with failing to document security requirements in contracts. |
| Part c | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT implements the acquisitions control through enforcement of the Office 365 Information Security Policy. The Office 365 Information Security Policy and associated standards (documented in the Active Framework Controls) 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 standards are addressed in the agreement, to provide a level of protection against identified risks equivalent to that provided by the Office 365 Information Security Policy.  It is the role of Corporate, External, & Legal Affairs (CELA) to approve all language included in system acquisition contracts pertaining to the security requirements. This includes the security functional requirements, security strength requirements, security assurance requirements, security-related documentation requirements, requirements for protecting security-related documentation, a description of the information system development environment and environment in which the system is intended to operate, and acceptance criteria, all of which are explained in detail in the documents mentioned above. Pre-existing third-party contracts are amended to include appropriate language upon renewal. This satisfies the acquisition control through effective management of the risks associated with failing to document security requirements in contracts. |
| Part d | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT implements the acquisitions control through enforcement of the Office 365 Information Security Policy. The Office 365 Information Security Policy and associated standards (documented in the Active Framework Controls) 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 standards are addressed in the agreement, to provide a level of protection against identified risks equivalent to that provided by the Office 365 Information Security Policy.  It is the role of Corporate, External, & Legal Affairs (CELA) to approve all language included in system acquisition contracts pertaining to the security requirements. This includes the security functional requirements, security strength requirements, security assurance requirements, security-related documentation requirements, requirements for protecting security-related documentation, a description of the information system development environment and environment in which the system is intended to operate, and acceptance criteria, all of which are explained in detail in the documents mentioned above. Pre-existing third-party contracts are amended to include appropriate language upon renewal. This satisfies the acquisition control through effective management of the risks associated with failing to document security requirements in contracts. |
| Part e | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT implements the acquisitions control through enforcement of the Office 365 Information Security Policy. The Office 365 Information Security Policy and associated standards (documented in the Active Framework Controls) 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 standards are addressed in the agreement, to provide a level of protection against identified risks equivalent to that provided by the Office 365 Information Security Policy.  It is the role of Corporate, External, & Legal Affairs (CELA) to approve all language included in system acquisition contracts pertaining to the security requirements. This includes the security functional requirements, security strength requirements, security assurance requirements, security-related documentation requirements, requirements for protecting security-related documentation, a description of the information system development environment and environment in which the system is intended to operate, and acceptance criteria, all of which are explained in detail in the documents mentioned above. Pre-existing third-party contracts are amended to include appropriate language upon renewal. This satisfies the acquisition control through effective management of the risks associated with failing to document security requirements in contracts. |
| Part f | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT implements the acquisitions control through enforcement of the Office 365 Information Security Policy. The Office 365 Information Security Policy and associated standards (documented in the Active Framework Controls) 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 standards are addressed in the agreement, to provide a level of protection against identified risks equivalent to that provided by the Office 365 Information Security Policy.  It is the role of Corporate, External, & Legal Affairs (CELA) to approve all language included in system acquisition contracts pertaining to the security requirements. This includes the security functional requirements, security strength requirements, security assurance requirements, security-related documentation requirements, requirements for protecting security-related documentation, a description of the information system development environment and environment in which the system is intended to operate, and acceptance criteria, all of which are explained in detail in the documents mentioned above. Pre-existing third-party contracts are amended to include appropriate language upon renewal. This satisfies the acquisition control through effective management of the risks associated with failing to document security requirements in contracts. |
| Part g | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT implements the acquisitions control through enforcement of the Office 365 Information Security Policy. The Office 365 Information Security Policy and associated standards (documented in the Active Framework Controls) 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 standards are addressed in the agreement, to provide a level of protection against identified risks equivalent to that provided by the Office 365 Information Security Policy.  It is the role of Corporate, External, & Legal Affairs (CELA) to approve all language included in system acquisition contracts pertaining to the security requirements. This includes the security functional requirements, security strength requirements, security assurance requirements, security-related documentation requirements, requirements for protecting security-related documentation, a description of the information system development environment and environment in which the system is intended to operate, and acceptance criteria, all of which are explained in detail in the documents mentioned above. Pre-existing third-party contracts are amended to include appropriate language upon renewal. This satisfies the acquisition control through effective management of the risks associated with failing to document security requirements in contracts. |

#### SA-4 (1) Control Enhancement (M) (H)

The organization requires the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed.

| SA-04(1) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Trust Program Manager, Program Manager | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SA-04(1) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The acquisition process described in SA-04 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 Office 365 MT service teams in their internal SharePoint sites.  Hardware acquisition is inherited from Azure, which has a FedRAMP IaaS P-ATO (package ID F1209051525). |

#### SA-4 (2) Control Enhancement (L) (M)

The organization requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed that includes: [FedRAMP Selection (one or more): to include security-relevant external system interfaces, and high-level design]; [Assignment: organization-defined design/implementation information] at [Assignment: organization-defined level of detail].

| SA-04(2) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Trust Program Manager, Program Manager | |
| Parameter SA-04(2):  1. security-relevant external system interfaces and high-level design; 2. 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SA-04(2) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The acquisition process described in SA-04 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 Office 365 MT service teams in their internal SharePoint sites.  Hardware acquisition is inherited from Azure, which has a FedRAMP IaaS P-ATO (package ID F1209051525). |

#### SA-4 (8) Control Enhancement (M) (H)

The organization requires the developer of the information system, system component, or information system service to produce a plan for the continuous monitoring of security control effectiveness that contains [FedRAMP Assignment: at least the minimum requirement as defined in control CA-7].

SA-4 (8) Additional FedRAMP Requirements and Guidance:

Guidance: CSP must use the same security standards regardless of where the system component or information system service is acquired.

| SA-04(8) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Trust Program Manager, Program Manager | |
| Parameter SA-04(8):  standards specified in continuous monitoring strategy documentation | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SA-04(8) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  As part of its continuous monitoring plan as outlined in the Office 365 Continuous Monitoring Strategy Guide, Office 365 MT continuously monitors control effectiveness of organizations that Office 365 MT inherits security controls from. |

#### SA-4 (9) Control Enhancement (M) (H)

The organization requires the developer of the information system, system component, or information system service to identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use.

| SA-04(9) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Trust Program Manager, Program Manager | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SA-04(9) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT includes as part of the design phase the identification of the functions, ports, protocols, and services intended for organizational use. |

#### SA-4 (10) Control Enhancement (M) (H)

The organization employs only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems.

| SA-04(10) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Trust Program Manager, Program Manager | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SA-04(10) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT does not implement PIV requirements for Government customers. As such, this control is not applicable. |

### SA-5 Information System Documentation (L) (M)

The organization:

1. Obtains administrator documentation for the information system, system component, or information system service that describes:
   1. Secure configuration, installation, and operation of the system, component, or service;
   2. Effective use and maintenance of security functions/mechanisms; and
   3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions;
2. Obtains user documentation for the information system, system component, or information system service that describes:
   1. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms;
   2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and
   3. User responsibilities in maintaining the security of the system, component, or service;
3. Documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and [Assignment: organization-defined actions] in response;
4. Protects documentation as required, in accordance with the risk management strategy; and
5. Distributes documentation to [Assignment: organization-defined personnel or roles)].

| SA-5 | Control Summary Information |
| --- | --- |
| Responsible Role: Azure, Office 365 Security Manager, Service Engineer Operations | |
| Parameter SA-05(c):  submits documentation to appropriate roles | |
| Parameter SA-05(e):  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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SA-5 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Part 1:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT 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. privileged) functions  This documentation is stored in each service team’s SharePoint site and made available to service team administrators.  Acquisition of hardware and associated documentation is inherited from Azure, which has a FedRAMP IaaS P-ATO (package ID F1209051525).  **Part 2:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT 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. privileged) functions  This documentation is stored in each service team’s SharePoint site and made available to service team administrators.  Acquisition of hardware and associated documentation is inherited from Azure, which has a FedRAMP IaaS P-ATO (package ID F1209051525).  **Part 3:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT 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. privileged) functions  This documentation is stored in each service team’s SharePoint site and made available to service team administrators.  Acquisition of hardware and associated documentation is inherited from Azure, which has a FedRAMP IaaS P-ATO (package ID F1209051525). |
| Part b | **Part 1:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT has extensive user-facing documentation on all aspects of the system, including security functions. This documentation is available online at: http://technet.microsoft.com/en-us/library/jj871004(v=office.15).aspx  **Part 2:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT has extensive user-facing documentation on all aspects of the system, including security functions. This documentation is available online at: http://technet.microsoft.com/en-us/library/jj871004(v=office.15).aspx  **Part 3:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT has extensive user-facing documentation on all aspects of the system, including security functions. This documentation is available online at: http://technet.microsoft.com/en-us/library/jj871004(v=office.15).aspx |
| Part c | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT documents failed attempts to acquire required documentation through use of the Office 365 Risk Management process. A ticket is opened to the Office 365 Risk Management team describing the documentation deficiency to Office 365 MT. The Office 365 Risk Management team will assess the risk this deficiency poses to Office 365 MT, develop a remediation plan appropriate to the level of risk (including opening a POA&M if required), and track the implementation of the remediation plan. |
| Part d | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT 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. privileged) functions  This documentation is stored in each service team’s SharePoint site and made available to service team administrators, developers, and testers. The documentation is secured via SharePoint's internal security mechanisms.  Acquisition of hardware and associated documentation is inherited from Azure which has a FedRAMP IaaS P-ATO (package ID F1209051525). |
| Part e | **Bing, Delve, DNS, EXO, IP, MSTeams, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT 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. privileged) functions  This documentation is stored in each service team’s SharePoint site and made available to service team administrators, developers, and testers. The documentation is secured via SharePoint's internal security mechanisms.  Acquisition of hardware and associated documentation is inherited from Azure which has a FedRAMP IaaS P-ATO (package ID F1209051525).  **OLM:**  Information system documentation is stored in confluence and can only be viewed by authorized user accounts. Documents in confluence are editable by everyone who has access and includes a change history. Different user groups in confluence have different permissions to prevent unauthorized access to documentation. |

### SA-8 Security Engineering Principles (M) (H)

The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.

| SA-08 | Control Summary Information |
| --- | --- |
| Responsible Role: Developer, Program Manager, Tester | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SA-08 - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT follows the process described in SA-03(a) for all phases in the lifecycle of the information system to ensure the application of security engineering principles.  The process is followed for all engineering initiatives associated with Office 365 MT. Additionally, associated standards (documented in the Active Framework Controls) provides details on how security should be built into information systems, software, and the development process. |

### SA-9 External Information System Services (L) (M) (H)

The organization:

1. Requires that providers of external information system services comply with organizational information security requirements and employ [FedRAMP Assignment: FedRAMP Security Controls Baseline(s) if Federal information is processed or stored within the external system] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
2. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and
3. Employs [FedRAMP Assignment: Federal/FedRAMP Continuous Monitoring requirements must be met for external systems where Federal information is processed or stored] to monitor security control compliance by external service providers on an ongoing basis.

Additional FedRAMP Requirements and Guidance

Guidance: See the FedRAMP Documents page under Key Cloud Service Provider (CSP) Documents> Continuous Monitoring Strategy Guide  
https://www.FedRAMP.gov/resources/documents

| SA-9 | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Trust Program Manager | |
| Parameter SA-09(a):  requirements defined in ISA when storing or processing customer content | |
| Parameter SA-09(c):  Federal/FedRAMP Continuous Monitoring 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SA-9 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Microsoft requires all third parties (external information system services) who are engaged with Office 365 to sign a Master Supplier Services Agreement (MSSA). The MSSA 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. Vendors that handle sensitive data must be in compliance with Microsoft vendor privacy practices and data protection requirements. Additionally, Office 365 MT signs Interconnection Security Agreements (ISAs) with external information systems as required by CA-03; ISAs define Office 365 MT oversight and roles/responsibilities.  The Office 365 MT Data Handling Standard maps “Federal information” to the categories “customer content” and “access control data”. Currently, Azure is the only Office 365 MT external information system service provider that stores or processes these categories. Azure has a FedRAMP P-ATO and is required to follow the FedRAMP security control baseline. |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT signs Interconnection Security Agreements (ISAs) with external information systems; ISAs define Office 365 MT oversight and roles/responsibilities. Agencies will receive and review ISAs as part of their authorization decision. Government oversight is performed by this agency review of Office 365 MT ISAs and continuous monitoring, which includes reports on ISA oversight. |
| Part c | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT compliance monitoring processes, methods and techniques are applied to customer content and access control data; are documented in ISAs; and are executed by Office 365 Trust. |

#### SA-9 (1) Control Enhancement (M) (H)

The organization:

1. Conducts an organizational assessment of risk prior to the acquisition or outsourcing of dedicated information security services; and
2. Ensures that the acquisition or outsourcing of dedicated information security services is approved by [Assignment: organization-defined personnel or roles].

| SA-9 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: None – Not Applicable | |
| Parameter SA-09(1)(b):  appropriate Service Engineer Operations 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SA-9 (1) - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT does not have any outsourced dedicated information security services. If any services were to be outsourced after receiving a FedRAMP P-ATO, Office 365 Trust would complete an assessment of risk and follow FedRAMP change management processes. |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  No acquisition or outsourcing of dedicated information security services is planned, but Office 365 MT will follow the FedRAMP change management process as part of continuous monitoring. |

**SA-9 (1) Additional FedRAMP Requirements and Guidance:**

**Requirement**: The service provider documents all existing outsourced security services and conducts a risk assessment of future outsourced security services. For JAB authorizations, future planned outsourced services are approved and accepted by the JAB.

| SA-09 (1) Req. | Control Summary Information |
| --- | --- |
| Responsible Role: Service Engineer Operations, Office 365 Security Manager | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SA-09 (1) Additional - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, SFB, SUE, OSI, SPO, SWE, WAC:**  Office 365 MT does not have any outsourced dedicated information security services. If any services were to be outsourced after receiving a FedRAMP P-ATO, Office 365 Trust would complete an assessment of risk and follow FedRAMP change management processes. |

#### SA-9 (2) Control Enhancement (M) (H)

The organization requires providers of [FedRAMP Assignment: All external systems where Federal information is processed or stored] to identify the functions, ports, protocols, and other services required for the use of such services.

| SA-09(2) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager, Service Engineer Operations | |
| Parameter SA-09(2):  all external information systems where customer content 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SA-09(2) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  As part of the process of establishing a connection to an external information system, Office 365 MT requires the system to provide information about the functions, ports, protocols and other services required for the use of such services. |

#### SA-9 (4) Control Enhancement (M) (H)

The organization employs [Assignment: organization-defined security safeguards] to ensure that the interests of [FedRAMP Assignment: All external systems where Federal information is processed or stored] are consistent with and reflect organizational interests.

| SA-09(4) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager, Service Engineer Operations | |
| Parameter SA-09(4):  1. FedRAMP security requirements; 2. all external systems where customer content 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SA-09(4) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Data Handling Standard maps “Federal information” to the categories “customer content” and “access control data”. Currently, Azure is the only Office 365 MT external information system service provider that stores or processes these categories. Azure has a FedRAMP P-ATO and is required to follow the FedRAMP security control baseline. |

#### SA-9 (5) Control Enhancement (M) (H)

The organization restricts the location of [FedRAMP Selection: information processing, information data, AND information services] to [Assignment: organization-defined locations] based on [Assignment: organization-defined requirements or conditions].

Additional FedRAMP Requirements and Guidance

Guidance: System services refer to FTP, Telnet, and TFTP, etc.

| SA-09(5) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager, Service Engineer Operations | |
| Parameter SA-09(5):  1. information processing, transmission information data, and information services; 2. Azure continental United States datacenters; 3. Office 365 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SA-09(5) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT restricts the location of all services and data within the accreditation boundary to Azure continental United States datacenters. When a government customer offering is purchased, the customer is provisioned into continental United States datacenters. |

### SA-10 Developer Configuration Management (M) (H)

The organization requires the developer of the information system, system component, or information system service to:

1. Perform configuration management during system, component, or service [FedRAMP Selection: development, implementation, AND operation];
2. Document, manage, and control the integrity of changes to [Assignment: organization-defined configuration items under configuration management];
3. Implement only organization-approved changes to the system, component, or service;
4. Document approved changes to the system, component, or service and the potential security impacts of such changes; and
5. Track security flaws and flaw resolution within the system, component, or service and report findings to [Assignment: organization-defined personnel].

SA-10 (e) Additional FedRAMP Requirements and Guidance:

Requirement: For JAB authorizations, track security flaws and flaw resolution within the system, component, or service and report findings to organization-defined personnel, to include FedRAMP ISSOs.

| SA-10 | Control Summary Information |
| --- | --- |
| Responsible Role: Developer, Office 365 Trust Program Manager, Program Manager, Tester | |
| Parameter SA-10(a):  development, implementation, and operation | |
| Parameter SA-10(b):  operational systems | |
| Parameter SA-10(e):  Office 365 Security Manager | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SA-10 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  All Office 365 MT software developers are required to follow the Office 365 Configuration Management Plan during information system design, development, implementation, and operation. |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT developers leverage ticketing tools or change management dashboards to document, manage and control the integrity of changes in the development environment. These tools and dashboards provide technical enforcement of documented change management processes. Among other features, they prevent changes to source code that are not tied to an approved change request. |
| Part c | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Developers of Office 365 MT implement only approved changes to the system. The service teams follow the configuration management processes when implementing changes. Changes are approved through ticketing tools or change management dashboards. |
| Part d | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The service team tracks all approved changes through ticketing tools or change management dashboards. As part of change management processes, other documentation such as the SSP or user and administrative documentation is updated if applicable. |
| Part e | **Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT service team developers track security flaws and flaw resolution during the development process using ticketing tools. Any identified flaws, whether discovered by a human or by the automated tools, have a corresponding bug opened. 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 and Office 365 Trust.  **Bing:**  If a security flaw is detected, the change cannot be submitted for review. Security flaws are detailed in build error logs that are available to Bing developers. Once the flaw is resolved, the change can be checked-in for review and tracked via a change management dashboard provided by PilotFish. |

#### SA-10 (1) Control Enhancement (M) (H)

The organization requires the developer of the information system, system component, or information system service to enable integrity verification of software and firmware components.

| SA-10(1) | Control Summary Information |
| --- | --- |
| Responsible Role: Developer, Office 365 Trust Program Manager, Program Manager, Tester | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SA-10(1) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT has determined that solutions to fully meet this control pose unacceptable risks to system availability. A complete discussion of these risks and the mitigating controls in place are documented in CM-7(2) decision log. |

### SA-11 Developer Security Testing and Evaluation (M) (H)

The organization requires the developer of the information system, system component, or information system service to:

1. Create and implement a security assessment plan;
2. Perform [Selection (one or more): unit; integration; system; regression] testing/evaluation at [Assignment: organization-defined depth and coverage];
3. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation;
4. Implement a verifiable flaw remediation process; and
5. Correct flaws identified during security testing/evaluation.

| SA-11 | Control Summary Information |
| --- | --- |
| Responsible Role: Developer, Office 365 Trust Program Manager, Program Manager, Tester | |
| Parameter SA-11(b):  1. unit, integration, system and regression; 2. static, dynamic and binary analysis which should be done in a white box or testing with full knowledge of the configuration and components used. Coverage will include all new services, components or systems being deployed and should include a report of the testing performed. | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SA-11 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Security testing occurs in several phases throughout the process. Specifically, security testing occurs during the following phases:  • Phase 3 – Implementation  • Phase 4 – Verification  • Phase 5 – Release  Microsoft, as part of its federal operations, will undergo a Security Testing and Evaluation (ST&E) process from an independent assessor. That assessor will perform a detailed evaluation based on NIST SP 800-53A, and as outlined in the Security Assessment Plan which will eventually be developed to support their test plan and procedures. |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT performs system, integration and regression security testing prior to release and before changes are made to existing features and functionality. |
| Part c | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The results of the security tests are documented in tickets opened in ticketing tools. Remediation work and successful retesting is documented in the same ticket. |
| Part d | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 MT system owner is responsible for ensuring that all system development and maintenance activities are performed.  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 ticketing tools 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 high vulnerabilities get remediated before the system will be released to production. A ticket for each vulnerability is opened in an automated ticketing tool and tracked to resolution. |
| Part e | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Flaws identified during testing are remediated prior to release. The results of the security tests are documented in tickets opened in ticketing tools. Remediation work and successful retesting is documented in the same ticket. |

#### SA-11 (1) Control Enhancement (M) (H)

The organization requires the developer of the information system, system component, or information system service to employ static code analysis tools to identify common flaws and document the results of the analysis.

SA-11 (1) Additional FedRAMP Requirements and Guidance:

Requirement: The service provider documents in the Continuous Monitoring Plan, how newly developed code for the information system is reviewed.

| SA-11(1) | Control Summary Information |
| --- | --- |
| Responsible Role: Developer, Tester | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SA-11(1) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Code reviews are performed, including use of the automated static code analysis tools. |

#### SA-11 (2) Control Enhancement (M) (H)

The organization requires the developer of the information system, system component, or information system service to perform threat and vulnerability analyses and subsequent testing/evaluation of the as-built system, component, or service.

| SA-11(2) | Control Summary Information |
| --- | --- |
| Responsible Role: Developer, Tester | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SA-11(2) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Security testing occurs in several phases. 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.  Threat analysis of the as-built system is performed as part of the Office 365 MT risk management process. |

#### SA-11 (8) Control Enhancement (M) (H)

The organization requires the developer of the information system, system component, or information system service to employ dynamic code analysis tools to identify common flaws and document the results of the analysis.

| SA-11(8) | Control Summary Information |
| --- | --- |
| Responsible Role: Developer, Tester | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SA-11(8) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Code reviews are performed, including use of unit testing and automated dynamic code analysis tools. |

* 1. System and Communications Protection (SC)

### SC-1 System and Communications Protection Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:

A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls; and

Reviews and updates the current:

System and communications protection policy [FedRAMP Assignment: at least every three (3) years]; and

System and communications protection procedures [FedRAMP Assignment: at least annually].

| SC-1 | Control Summary Information |
| --- | --- |
| Responsible Role: Service Engineer Operations | |
| Parameter SC-01(a)(1):  Service Engineer Operations, Program Manager, Developer, Tester, Office 365 Trust Program Manager, Office 365 Security Manager, BCM | |
| Parameter SC-01(a)(2):  Service Engineer Operations, Program Manager, Developer, Tester, Office 365 Trust Program Manager, Office 365 Security Manager, BCM | |
| Parameter SC-01(b)(1):  annually | |
| Parameter SC-01(b)(2):  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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SC-1 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Part 1:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Information Security Policy defines Office 365 MT policies. This document addresses the purpose, scope, roles, responsibilities, compliance requirements, and required coordination among the various Microsoft organizations providing some level of support for the security of Office 365 MT. Policies are made available to roles providing support for Office 365 system and communications protection via SharePoint.  **Part 2:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Information Security Policy contains policies that must be met in the delivery and operation of Office 365 MT. Standards and Procedures to facilitate execution of these policies are documented in the Active Framework Controls, Office 365 Standard Operating Procedures (SOPs), and service team-specific SOPs. These standards and procedures act as adjuncts to the security policy and provide implementation level requirements and details to carry out specific operational tasks. A detailed mapping of Office 365 Standards and Procedures to each control is available. Office 365 SOPs are distributed to roles providing support for system and communications protection via SharePoint. |
| Part b | **Part 1:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Information Security Policy is reviewed and updated annually by the Office 365 Trust team.  **Part 2:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 SOPs are reviewed and updated annually by the service teams and by Office 365 Trust. |

### SC-2 Application Partitioning (M) (H)

The information system separates user functionality (including user interface services) from information system management functionality.

| SC-02 | Control Summary Information |
| --- | --- |
| Responsible Role: 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SC-02 - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT achieves application partitioning by utilizing three distinct groups of roles for accessing system functionality. These groups of roles are segregated using Active Directory (AD). These roles are described as follows:  • Administrative Backend – This group is where Office 365 MT administrators manage the Operating System-level functions and systems. No Office 365 MT customer user or customer administrator has access to these functions, as it is strictly provisioned for those managing the underlying technologies that support the Office 365 MT infrastructure.  • Customer Administration – This group is where administrators from the customer side have the ability to customize the experience and configurations for the customer users of Office 365 MT for their specific organization. Other limited configuration options are provided as a part of the Office 365 MT service which is restricted to customer administrators. These interfaces are specifically restricted to customer administrators.  • Customer User Level Access – This role is strictly for providing access to the Office 365 MT service for functions used by the customer users, for example for customer users to access Exchange Online and SharePoint Online.  Office 365 MT employs customer-facing software for use by customers, and administrative OS functions to be carried out by Office 365 MT administrators. Active Directory restrictions are put into place to prevent a customer user from being able to access any customer administration or Office 365 MT administrative backend functions. Customer users, customer administrators, and Office 365 MT administrators are completely segregated from each other and are not able to access resources outside of their respective designated roles. |

### SC-4 Information in Shared Resources (M) (H)

The information system prevents unauthorized and unintended information transfer via shared system resources.

| SC-04 | Control Summary Information |
| --- | --- |
| Responsible Role: Customer Administrator, MSIT, Office 365 Security Manager | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SC-04 - What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility:**  Government customers are responsible for only sharing government customer content with properly authenticated government customer users. There are two mechanisms by which government customers could potentially share government customer content with non-authorized users: guest access to SFB meetings and SharePoint Online guest access.  Guest access to SFB meetings, if enabled, allows anyone with a meeting invite to access the meeting lobby. The meeting organizer is responsible for establishing the identity of lobby participants before granting them access to the meeting. Government customers are responsible for disabling guest access to SFB meetings to remain compliant with FedRAMP standards as advised in "Office 365 MT Government Compliance Considerations v 2 00".  Non-government customers are responsible for determining if the use of guest access to SFB meetings should be allowed for their organization. This setting can be configured by government and non-government customers. For more information, see the following TechNet article: http://technet.microsoft.com/en-US/library/gg398648.aspx  SharePoint Online guest invitations allow external users to access an organization’s SharePoint site(s). Government and non-government customers are responsible for determining if the use of guest access to SharePoint Online, as an account type, should be allowed for their organization. Government customers are responsible for disabling guest access to SharePoint Online to remain compliant with FedRAMP standards as advised in "Office 365 MT Government Compliance Considerations v 2 00".  The setting to allow or disallow guest access to SharePoint Online can be configured by government and non-government customers. For more information, see the following Office 365 MT help article: http://office.microsoft.com/en-us/office365-sharepoint-online-small-business-help/manage-sharing-with-external-users-HA102849862.aspx  Government customers are responsible for ensuring that no information with a security impact level greater than moderate is stored, processed, or transmitted via the services provided to them by Office 365.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  A detailed list of specific technical mechanisms implemented within Office 365 MT to prevent unauthorized and unintended information transfer via shared system resources is documented in "Microsoft Office 365 Tenant Separation". Shared resources in Office 365 MT require each Office 365 MT user (including Office 365 service team administrators, customer administrators, and customer users) to hold a unique Active Directory (AD) identifier. Access to shared resources is governed by explicit access allocation, and information is segregated between Office 365 MT user sessions through AD and Azure Active Directory (AAD). |

### SC-5 Denial of Service Protection (L) (M) (H)

The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined types of denial of service attacks or reference to source for such information] by employing [Assignment: organization-defined security safeguards].

| SC-05 | Control Summary Information |
| --- | --- |
| Responsible Role: Azure | |
| Parameter SC-05:  1. single point and distributed network flooding denial of service attacks; 2. anomaly detection and mitigation using OneDDOS, as well as redundant server implementation within mirrored active/active data centers | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SC-05 - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Azure implements OneDDOS for the Office 365 MT service teams as defense against single point and distributed network flooding denial of service attacks. Individual service teams request OneDDOS deployment from Azure.  OneDDOS is a solution for network-wide, non-intrusive reporting, anomaly detection and intelligent mitigation. Using flow data, SNMP and BGP updates, OneDDOS learns normal traffic and routing behavior across hundreds of routers and thousands of interfaces, and correlates the traffic patterns with the topology data to build logical data models. This information enables network and security operations staff to detect and mitigate threats to availability, improve network/service performance and make better investment decisions concerning capacity planning, service offerings and traffic management.  In addition, service teams use redundant server implementation within each data center as well as mirrored active/active data centers to enhance availability of services. Microsoft requires planning for software/logic-based denial of service attacks and minimizing their potential effects. |

### SC-6 Resource Availability (M) (H)

The information system protects the availability of resources by allocating [Assignment: organization-defined resources] by [Selection (one or more); priority; quota; [Assignment: organization-defined security safeguards]].

| SC-06 | Control Summary Information |
| --- | --- |
| Responsible Role: Service Engineer Operations | |
| Parameter SC-06:  1. processor and memory resources; 2. process priority; per-tenant utilization quota | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SC-06 - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Microsoft requires consideration of situations where the system may be threatened by resource overutilization. In these cases, the Office 365 MT servers are configured to limit the use of processor and memory resources by process priority. This is a built-in feature of the Windows OS. Additionally, service teams monitor processor and memory utilization spikes and initiate the incident response process if spikes threaten the health of Office 365 MT. Also, process and memory resources are capped per tenant, which prevents any single tenant from interfering with the availability of other tenant’s services. |

### SC-7 Boundary Protection (L) (M) (H)

The information system:

1. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; and
2. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and
3. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with organizational security architecture.

| SC-7 | Control Summary Information |
| --- | --- |
| Responsible Role: Customer Administrator, Azure, Office 365 Security Manager, Service Engineer Operations | |
| Parameter SC-07(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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SC-7 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT monitors and controls communications at the external boundary of the system and at key internal boundaries within the system through the use of controlled devices at the network boundary and at key points within the network. The overarching principle of network security is to allow only connection and communication that is necessary to allow systems to operate, blocking all other ports, protocols and connections by default. Access Control Lists (ACLs) are the preferred mechanism through which 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, firewall rules, and host-based firewall rules. |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The only publicly-accessible components of Office 365 MT are the load balancers and the public-facing server roles. All non-publicly-accessible Office 365 MT components connect to the load balancers via physically-separate network interfaces on subnets that are logically separated from internal subnets. |
| Part c | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT connects to external networks or information systems only through Azure-managed networks. The network interfaces provide boundary protection using tiered Access Control Lists (ACLs) and are arranged in accordance with organizational security architecture. Pre-approved communications are described by Azure as follows:  The ingress ACL applies to network traffic as it enters a subnet; the point of implementation of the ACL is the gateway interface(s) of the subnet. Ingress ACLs permitting network traffic to cross between different Properties, Environments, or AD Domains are more restrictive than ACLs permitting network traffic within the same Property, Environment, and AD Domain; these restrictions are labeled accordingly. |

#### SC-7 (3) Control Enhancement (M) (H)

The organization limits the number external network connections to the information system.

| SC-07(3) | Control Summary Information |
| --- | --- |
| Responsible Role: Azure, Office 365 Security Manager | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SC-07(3) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  All inbound and outbound traffic is controlled and monitored through a limited number of network access points at the boundary and at key points within the system. Service team connections into the environment are restricted and controlled through Terminal Server Gateways (TSGs). Each service team has one or more groups of TSGs behind a load balancer to limit the access points for administration traffic, and customer traffic passes through a load balancer as well. All entry points are monitored and generate audit logs and alerts in real time. |

#### SC-7 (4) Control Enhancement (M)

The organization:

1. Implements a managed interface for each external telecommunication service;

Establishes a traffic flow policy for each managed interface;

Protects the confidentiality and integrity of the information being transmitted across each interface;

Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and

1. Reviews exceptions to the traffic flow policy [FedRAMP Assignment: at least at least annually] and removes exceptions that are no longer supported by an explicit mission/business need.

| SC-7 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: Azure, Office 365 Security Manager | |
| Parameter SC-07(4)(e):  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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SC-7 (4) - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT implements managed interfaces using Access Control Lists (ACLs). ACLs are the preferred mechanism through which to restrict network communications by source and destination networks, protocols, and port numbers and are managed by Azure and the Office 365 MT service teams. Service teams work with Azure to establish individual access rules. See the Azure SSP and AC-04 in this SSP for additional details. |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT maintains a documented, approved traffic flow policy for managed interfaces (deny all, permit by exception). The Office 365 Security team is responsible for approving and monitoring exceptions to the Firewall Rule and Tiered ACL Guidelines document. |
| Part c | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT uses ACLs and encryption to protect the confidentiality and integrity of data being transmitted across each interface. Approved mechanisms to implement networked-based ACLs are: ACLs on routers and network firewall rules managed by Azure, and host-based firewall rules.  Office 365 MT service teams also implement encryption mechanisms on all communications between interconnected systems and between customers. All encryption modules are operated in compliance with FIPS 140-2. This ensures the confidentiality and integrity of communications between service teams, interconnected systems, and customers are protected. |
| Part d | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT maintains a deny all, permit by exception traffic flow policy for all service teams. Exceptions to the traffic flow policy and changes to the exception list are based on operational needs. Changes are requested through ticketing tools and must be approved by the Change Advisory Board (CAB) and are reviewed annually as described in part e of this control. |
| Part e | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Exceptions to traffic flow policy are reviewed by service teams at least annually as part of the data flow diagram review process managed by Office 365 Trust.  After traffic flow policy review, any rules that are determined to be no longer needed to support an explicit mission/business need are removed. Requests for removal follow the same process as requests to add rules. |

#### SC-7 (5) Control Enhancement (M) (H)

The information system at managed interfaces denies network traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception).

| SC-07(5) | Control Summary Information |
| --- | --- |
| Responsible Role: Azure, Office 365 Security Manager | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SC-07(5) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT has implemented a deny-by-default policy and only allows connections by exception. This policy is enforced by network access control list (ACL) rules on devices in the boundary. |

#### SC-7 (7) Control Enhancement (M) (H)

The information system, in conjunction with a remote device, prevents the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks.

| SC-07(7) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869) | |

| SC-07(7) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT does not allow Virtual Private Network (VPN) connections into the environment. All administrative remote access to Office 365 MT is terminated at the Terminal Server Gateways (TSGs). Access to the TSGs is remote; there is no VPN network connectivity between the remote device and Office 365 MT networks. The remote device only has access to a remote desktop session terminated at the TSG and therefore there is no capability to bridge the connection to an external network. |

#### SC-7 (8) Control Enhancement (M) (H)

The information system routes [Assignment: organization-defined internal communications traffic] to [Assignment: organization-defined external networks] through authenticated proxy servers at managed interfaces.

| SC-07(8) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager | |
| Parameter SC-07(8):  1. defines the internal communications traffic to be routed by the information system through authenticated proxy servers; Personnel with two factor authentication and AD permission to the TSGs; 2. external networks that are the prospective destination of such traffic routing; There are no external networks | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SC-07(8) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT routes all communication with external networks through a limited number of access points at the boundary. Thus, Office 365 MT does not make use of proxy servers, web content filtering, or traditional proxy functions. |

#### SC-7 (12) Control Enhancement (M)

The organization implements [*Assignment: organization-defined host-based boundary protection mechanisms*] at [Assignment: organization-defined information system components].

| SC-07(12) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager, Service Engineer Operations | |
| Parameter SC-07(12):  1. host-based boundary protection through the use of the Windows firewall; 2. all servers in Office 365 | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SC-07(12) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, SFB, OLM, OSI, SUE, SWE, WAC:**  Office 365 MT has implemented host-based boundary protection using Windows Firewall throughout the environment. Windows machines have implemented host-based boundary protection using Windows Firewall. Office 365 Security PAVC scanning mechanisms ensure the Windows Firewall is enabled.  For teams using Linux workstations, host-based boundary protection is implemented through Azure network security group (NSG) rules or by configuring the Iptables command line utility.  **SPO:**  POA&M MT-0075 has been created to track the implementation of host-based firewalls for SPO. |

#### SC-7 (13) Control Enhancement (M)

The organization isolates [FedRAMP Assignment: See SC-7 (13) additional FedRAMP Requirements and Guidance] from other internal information system components by implementing physically separate subnetworks with managed interfaces to other components of the system.

SC-7 (13) Additional FedRAMP Requirements and Guidance:

Requirement: The service provider defines key information security tools, mechanisms, and support components associated with system and security administration and isolates those tools, mechanisms, and support components from other internal information system components via physically or logically separate subnets.

| SC-07(13) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Trust Program Manager | |
| Parameter SC-07(13):  Security alerting tools, PAVC, TSGs, incident management 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SC-07(13) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Azure clusters or the Security Workload Environment (SWE) isolates security tools/mechanisms, PAVC, automated security alerting tools, TSGs, and Incident management systems from the rest of Office 365 MT by implementing physically separate subnetworks with managed interfaces to other components of the system. |

#### SC-7 (18) Control Enhancement (M) (H)

The information system fails securely in the event of an operational failure of a boundary protection device.

| SC-07(18) | Control Summary Information |
| --- | --- |
| Responsible Role: Azure, Office 365 Security Manager | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SC-07(18) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT boundary protection devices implemented by Azure are all in multi-redundant configurations. By default, any failure of one device triggers failover to a backup, equally secure device. If this process fails or the backup fails, all mechanisms are configured to fail closed, disconnecting all access to Office 365 MT and preventing any loss of data confidentiality or integrity. |

### SC-8 Transmission confidentiality and Integrity (M) (H)

The information system protects the [FedRAMP Assignment: confidentiality AND integrity] of transmitted information.

| SC-08 | Control Summary Information |
| --- | --- |
| Responsible Role: Customer Administrator, Azure, Office 365 Security Manager, Service Engineer Operations | |
| Parameter SC-08:  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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SC-08 - What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility:**  Government customers are responsible for having a process in place to check the validity of the Office 365 Web sites prior to signing on by reviewing the digital certificate on the site to ensure they are the Office 365 Web sites. 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.  Government customers are responsible for ensuring that client software is configured to only establish sessions using FIPS 140-2 compliant protocols. This can be accomplished by restricting access to the government customer’s ADFS to only internal network traffic. This will force government customers attempting to connect to Office 365 MT to VPN into the customer’s network or directly be on the network at the time of authentication. When the customer connects (directly or via VPN) to the network it should perform a health inspection that validates USGCB baselines including browser settings to require FIPS 140-2 connections. For more information about configuring customer ADFS server(s) to only allow connections from customer internal networks, see the following TechNet article: http://technet.microsoft.com/en-us/library/hh526961(v=ws.10).aspx  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT uses encryption to protect the integrity and confidentiality of transmitted information. Specifically, Office 365 MT provides FIPS 140-2 compliant cipher support for customer connections, interconnected system connections, and remote access connections to Office 365 MT.  For connections to customers, Office 365 MT is configured to negotiate FIPS compliant TLS protocols with supported client browsers, though non-FIPS compliant protocols are supported for legacy browser support.  Remote access connections from Office 365 MT service team users are made using strictly enforced FIPS compliant TLS protocols.  Office 365 MT’s FIPS 140-2 encryption modules used for transmitted information are certified by NIST via certificates 1334, 1335, and 1336. |

#### SC-8 (1) Control Enhancement (M) (H)

The information system implements cryptographic mechanisms to [FedRAMP Assignment: prevent unauthorized disclosure of information AND detect changes to information] during transmission unless otherwise protected by [FedRAMP Assignment: a hardened or alarmed carrier Protective Distribution System (PDS)].

| SC-08(1) | Control Summary Information |
| --- | --- |
| Responsible Role: Azure, Office 365 Security Manager, Service Engineer Operations | |
| Parameter SC-08(1):  1. prevent unauthorized disclosure of information and detect changes to information; 2. a hardened or alarmed carrier Protective Distribution System (PDS) | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SC-08(1) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT uses encryption to prevent unauthorized disclosure of information and detect changes to information during transmission. Specifically, Office 365 MT provides FIPS 140-2 compliant ciphers that include integrity validation for customer connections, interconnected system connections, and remote access connections to Office 365 MT.  For connections to customers, Office 365 MT is configured to negotiate FIPS compliant TLS protocols with supported client browsers, though non-FIPS compliant protocols are supported for legacy browser support.  Connections to interconnected systems are made using strictly enforced FIPS compliant TLS protocols.  Remote access connections from Office 365 MT service team users are made using strictly enforced FIPS compliant TLS protocols.  Office 365 MT’s FIPS 140-2 encryption modules used for transmitted information are certified by NIST via certificates 1334, 1335, and 1336. |

### SC-10 Network Disconnect (M)

The information system terminates the network connection associated with a communications session at the end of the session or after [FedRAMP Assignment: no longer than thirty (30) minutes for RAS-based sessions and no longer than sixty (60) minutes for non-interactive user sessions] of inactivity.

| SC-10 | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager, Service Engineer Operations | |
| Parameter SC-10:  30 minutes for all RAS-based sessions; 30 to 60 minutes for non-interactive users (Note: Long running batch jobs and other operations are not subject to this time limit) | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SC-10 - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT terminates the network connection associated with a communications session at the end of the session or after 30 minutes of inactivity. |

### SC-12 Cryptographic Key Establishment & Management (L) (M) (H)

The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].

SC-12 Additional FedRAMP Requirements and Guidance:

Guidance: Federally approved and validated cryptography.

| SC-12 | Control Summary Information |
| --- | --- |
| Responsible Role: Customer Administrator, Office 365 Security Manager, Service Engineer Operations | |
| Parameter SC-12:  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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SC-12 - What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility:**  Government customers, by agreeing to policies upon signing on to use the system, will not enable any SharePoint Online functionality (SharePoint Lite / SharePoint Vanity Domains) that bypasses network-level encryption.  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.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  In accordance with the Public Key Infrastructure Operational Security Standard, Office 365 leverages the cryptographic capabilities that are directly a part of the Windows Operating System for certificates and authentication mechanisms (e.g. Kerberos). These cryptographic modules have been certified by NIST as being FIPS 140-2 complaint. OLM employs Device Bundle Encryption for their frontend and Account Bundle Encryption for their backend which both use an AES128 symmetric keys, and utilizes Azure KeyVault for key management.  Relevant NIST certificate numbers are: 1321, 1333, 1334, 1335, 1336, and 1339. Any time cryptographic capabilities are employed to protect the confidentiality, integrity, or availability of data within Office 365 MT, the modules and ciphers used are FIPS 140-2 compliant. |

#### SC-12 (2) Control Enhancement (M) (H)

The organization produces, controls, and distributes symmetric cryptographic keys using [FedRAMP Selection: NIST FIPS-compliant] key management technology and processes.

| SC-12(2) | Control Summary Information |
| --- | --- |
| Responsible Role: Customer Administrator | |
| Parameter SC-12(2):  NIST-Approved | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SC-12(2) - What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility:**  Government Office 365 MT customers are not required to use symmetric cryptographic keys, but should they choose to, they are responsible for producing, controlling, and distributing symmetric cryptographic keys using NIST FIPS-Validated key management technology and processes.  Non-government customers of Office 365 MT are not required to use symmetric cryptographic keys, but should they choose to, they are responsible for producing, controlling, and distributing symmetric cryptographic keys using NIST FIPS-Validated key management technology and processes.  **Delve, DNS, EXO, IP, MSTeams, OSI, SFB, SWE, WAC:**  Office 365 MT does not produce, control, or distribute symmetric cryptographic keys.  **OLM, SPO:**  OLM and SPO use AES256 symmetric keys to perform logical (per-file) encryption of content at rest. SPO stores content keys to the SharePoint Online Content Database within the SPO MT environment, and the content keys are created and deleted along with the associated content. Any time cryptographic capabilities are employed to protect the confidentiality, integrity, or availability of data within Office 365 MT, the modules and ciphers used are FIPS 140-2 compliant. In addition to encryption inherited from Azure, OLM uses Use of Device Bundle Encryption and Account Bundle Encryption and uses Azure KeyVault for key management. For additional information on how cryptographic modules are employed in Microsoft products, see TechNet article cc750357: http://technet.microsoft.com/en-us/library/cc750357.aspx  **Bing, SUE:**  Symmetric keys are used internally and are produced, controlled and distributed in accordance with Microsoft cryptographic policies. |

#### SC-12 (3) Control Enhancement (M) (H)

The organization produces, controls, and distributes asymmetric cryptographic keys using [Selection: NSA-approved key management technology and processes; approved PKI Class 3 certificates or prepositioned keying material; approved PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user’s private key].

| SC-12(3) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager, Service Engineer Operations | |
| Parameter SC-12(3):  approved PKI Class 3 certificates | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SC-12(3) - What is the solution and how is it implemented? |
| --- |
| **EXO, IP:**  Office 365 MT produces, controls, and distributes asymmetric cryptographic keys using approved PKI Class 3 certificates. Asymmetric key generation is initiated within Central Admin in the capacity forest where the corresponding certificate will be validated. A public-private key pair is generated by Central Admin. The private key is immediately encrypted and stored in the Central Admin secret store; it is never transmitted outside the boundary and the Central Admin secret store will not allow the private key to be viewed or exported. The Central Admin secret store will only allow the private key to be used to sign requests via API. The corresponding public key is placed in a CER file, which is sent to SSLAdmin via a FIPS 140-2 compliant TLS 1.2 internal network connection. SSLAdmin then signs the public key with its root certificate and returns the signed public key for distribution.  **Bing, Delve, DNS, MSTeams, OLM, OSI, SFB, SUE, SWE, WAC:**  Office 365 MT produces, controls, and distributes asymmetric cryptographic keys using approved PKI Class 3 certificates. Signed certificates are obtained from SSLAdmin. Specifically, key generation is initiated on the servers that are to have keys installed. The public key is sent to SSLAdmin, which then in turn creates the public key CER file. The CER file is then copied to the server over a secured internal network. Once the CER file is received, the PFX (complete key) file is created by combining the private key with the CER file. The PFX file is copied over secure networks to cluster nodes. Once installation is complete the PFX key is then deleted from all servers involved in key creation and stored in SCRAM or SecureValues.  **SPO:**  Office 365 MT produces, controls, and distributes asymmetric cryptographic keys using approved PKI Class 3 certificates. Signed certificates are obtained from SSLAdmin. Specifically, key generation is initiated on the SPO Crypto Server in Corpnet. The public key is sent to SSLAdmin, which then in turn creates the public key CER file. The CER file is then copied to the server over a secured internal network. Once the CER file is received, the PFX (complete key) file is created by combining the private key with the CER file. The PFX file is copied over secure networks to a secret store within the environment, to be installed. Once installation is complete the PFX key is then deleted from all servers involved in key creation. |

### SC-13 Use of Cryptography (L) (M) (H)

The information system implements [FedRAMP Assignment: FIPS-validated or NSA-approved cryptography] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

| SC-13 | Control Summary Information |
| --- | --- |
| Responsible Role: Customer Administrator, Office 365 Security Manager, Service Engineer Operations | |
| Parameter SC-13:  FIPS 14N/A-2, Web references: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm, www.cnss.gov | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SC-13 - What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility:**  Government customers are responsible for ensuring that client software is configured to only establish sessions using FIPS 140-2 compliant protocols. This can be accomplished by restricting access to the government customer’s ADFS to only internal network traffic. This will force government customers attempting to connect to Office 365 MT to VPN into the customer’s network or directly be on the network at the time of authentication. When the customer connects (directly or via VPN) to the network it should perform a health inspection that validates USGCB baselines including browser settings to require FIPS 140-2 connections. For more information about configuring customer ADFS server(s) to only allow connections from customer internal networks, see the following TechNet article: http://technet.microsoft.com/en-us/library/hh526961(v=ws.10).aspx  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Encryption mechanisms and techniques used by the service teams follow the requirements and restrictions outlined in the Office 365 Information Security Policy and associated standards (documented in the Active Framework Controls). Service data and information are handled in accordance with the requirements and restrictions specified in the Enterprise Online Services Data Taxonomy document when cryptography is used. The Enterprise Online Services Data Taxonomy document establishes the mandatory minimum requirements for Office 365 asset ownership, classification, and protection.  Office 365 MT leverages the cryptographic capabilities that are directly a part of the Windows operating system for certificates and authentication mechanisms such as Kerberos. These cryptographic modules have been certified by NIST as being FIPS 140-2 complaint. Relevant NIST certificate numbers are: 1321, 1333, 1334, 1335, 1336, and 1339. Any time cryptographic capabilities are employed to protect the confidentiality, integrity, or availability of data within Office 365, the modules and ciphers are FIPS 140-2 compliant.  OLM uses an AES128 symmetric keys to perform logical (per-file) encryption of content at rest. Any time cryptographic capabilities are employed to protect the confidentiality, integrity, or availability of data within the OLM environment, the modules and ciphers used are FIPS 140-2 compliant. For additional information on how cryptographic modules are employed in Microsoft products, see TechNet article cc750357: http://technet.microsoft.com/en-us/library/cc750357.aspx |

### SC-15 Collaborative Computing Devices (M) (H)

The information system:

1. Prohibits remote activation of collaborative computing devices with the following exceptions: [FedRAMP Assignment: no exceptions] and
2. Provides an explicit indication of use to users physically present at the devices.

| SC-15 | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager, Service Engineer Operations | |
| Parameter SC-15(a):  no exceptions allowed | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SC-15 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SPO, SUE, SWE, WAC:**  The above Office 365 MT systems do not support collaborative computing devices in production environments.  **SFB:**  The Microsoft SFB product does not support remote activation of sessions. The session initiator sends a request to connect, and the receiving user must accept that incoming request for a session to begin. | |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SPO, SUE, SWE, WAC:**  The above Office 365 MT systems do not support collaborative computing devices in production environments.  **SFB:**  The SFB client explicitly signals users through use of audible alerts and on-screen messages to indicate attempts to initiate remote communication sessions. | |

SC-15 Additional FedRAMP Requirements and Guidance:

Requirement: The information system provides disablement (instead of physical disconnect) of collaborative computing devices in a manner that supports ease of use.

| SC-15 Req. | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SC-15 Req. - What is the solution and how is it implemented? | |
| --- | --- |
| Req. 1 | **Customer Responsibility:**  Physical devices used to support SFB sessions by customers, such as end user laptops, are outside of the boundary of Office 365 MultiTenant Cloud. It is the responsibility of customers to ensure that end user laptops and other physical devices support "disablement" of collaborative computing features.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The above Office 365 systems do not support collaborative computing devices in the production environments. |

### SC-17 Public Key Infrastructure Certificates (M) (H)

The organization issues public key certificates under an [Assignment: organization-defined certificate policy] or obtains public key certificates from an approved service provider.

| SC-17 | Control Summary Information |
| --- | --- |
| Responsible Role: Customer Administrator, Office 365 Security Manager, Service Engineer Operations | |
| Parameter SC-17:  Microsoft PKI policy | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SC-17 - What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility:**  Government customers are responsible for having a process in place to check the validity of the Office 365 Web sites prior to signing on by reviewing the digital certificate on the site to ensure they are the Office 365 Web sites. 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.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Microsoft’s corporate Public Key Infrastructure (PKI) has been established to provide a variety of digital certificate services to support operations for Office 365 MT and for the Microsoft Corporation. Microsoft corporate PKI functions as the Certificate Authority and Registration Authority and provides directory services to manage keys and certificates. These functions are conducted in accordance with the Public Key Infrastructure Operational Security Standard, which is a component of Microsoft PKI Requirements. |

### SC-18 Mobile Code (M) (H)

The organization:

1. Defines acceptable and unacceptable mobile code and mobile code technologies;
2. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and
3. Authorizes, monitors, and controls the use of mobile code within the information system.

| SC-18 | Control Summary Information |
| --- | --- |
| Responsible Role: Developer, Program Manager, Tester | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SC-18 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT defines acceptable and unacceptable mobile code technologies by evaluating and approving each use of mobile code independently. If a requirement for use of mobile code in the application is identified by a service team during the requirements phase, this requirement is then included in the security section of the Feature and Design Spec documents, which must be approved before the mobile code technology is considered approved. Unapproved mobile code is any mobile code that has not been developed and approved. |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  All approved mobile code in use in the environment is developed and reviewed. All releases have release-specific implementation guidance and testing to ensure that only acceptable code is released. |
| Part c | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT authorizes, monitors, and controls the use of mobile code developed by the service teams, including peer review and the Security Code Review, to detect the presence of unauthorized mobile code. |

### SC-19 Voice Over Internet Protocol (M) (H)

The organization:

1. Establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and
2. Authorizes, monitors, and controls the use of VoIP within the information system.

| SC-19 | Control Summary Information |
| --- | --- |
| Responsible Role: Customer Administrator, 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SC-19 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility:**  Government customers are responsible for secure use of the VoIP functions provided by SFB. SFB is default configured to enforce FIPS 140-2 validated encryption for VoIP connection initiation on ports 5060 and 5061, and it is the responsibility of the government customer not to change these configuration settings at the client level. These settings can be enforced by restricting access to the government customer’s ADFS to only internal network traffic. This will force government customers attempting to connect to Office 365 MT to VPN into the customer’s network or directly be on the network at the time of authentication. When the customer connects (directly or via VPN) to the network it should perform a health inspection that validates SFB client configurations. For more information about configuring customer ADFS server(s) to only allow connections from customer internal networks, see the following TechNet article: http://technet.microsoft.com/en-us/library/hh526961(v=ws.10).aspx  **Bing, Delve, DNS, IP, MSTeams, OLM, OSI, SPO, SUE, SWE, WAC:**  Voice over Internet Protocol is not authorized in these software components.  **EXO:**  While Exchange Online (EXO) Unified Messaging (UM) provides VoIP services as an option, it is the responsibility of the customer to determine if allowing use of these services presents a risk to the customer. Microsoft makes UM usage information available to the customer to aid in monitoring and controlling the use of VoIP should the customer choose to use this feature.  **SFB:**  SFB enables customers to place VoIP calls using the SFB client. Customers are responsible for making the decision to authorize this use. SFB monitors and controls authorized VoIP use equivalently to all Office 365 MT customer content. |
| Part b | **Customer Responsibility:**  Government customers are responsible for secure use of the VoIP functions provided by SFB. SFB is default configured to enforce FIPS 140-2 validated encryption for VoIP connection initiation on ports 5060 and 5061, and it is the responsibility of the government customer not to change these configuration settings at the client level. These settings can be enforced by restricting access to the government customer’s ADFS to only internal network traffic. This will force government customers attempting to connect to Office 365 MT to VPN into the customer’s network or directly be on the network at the time of authentication. When the customer connects (directly or via VPN) to the network it should perform a health inspection that validates SFB client configurations. For more information about configuring customer ADFS server(s) to only allow connections from customer internal networks, see the following TechNet article: http://technet.microsoft.com/en-us/library/hh526961(v=ws.10).aspx  **Bing, Delve, DNS, IP, MSTeams, OLM, OSI, SPO, SUE, SWE, WAC:**  Voice over Internet Protocol is not authorized in these software components.  **EXO:**  Exchange Online (EXO) authorizes Unified Message (UM) if the customer specifically requests use of VoIP. All calls are logged to the standard described in the AU control family.  **SFB:**  SFB enables customers to place VoIP calls using the SFB client. Customers are responsible for making the decision to authorize this use. SFB monitors and controls authorized VoIP use equivalently to all Office 365 MT customer content. |

### SC-20 Secure Name / Address Resolution Service (Authoritative Source) (L) (M) (H)

The information system:

1. Provides 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

Provides 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.

| SC-20 | Control Summary Information |
| --- | --- |
| Responsible Role: None – 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869) | |

| SC-20 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  OMB Memorandum 08-23 specifies that DNS providers must take certain actions to protect .gov domains. Microsoft does not resolve .gov domain names for Federal users, so this control is not applicable. |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  OMB Memorandum 08-23 specifies that DNS providers must take certain actions to protect .gov domains. Microsoft does not resolve .gov domain names for Federal users, so this control is not applicable. |

### SC-21 Secure Name / Address Resolution Service (Recursive or Caching Resolver) (L) (M) (H)

The information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

| SC-21 | Control Summary Information |
| --- | --- |
| Responsible Role: None – 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869) | |

| SC-21 - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  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.  Office 365 MT internal DNS servers resolve DNS queries from Office 365 MT servers. Office 365 MT 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.  Office 365 DNS's production servers act as authoritative sources for DNS requests from external clients for various Office 365 MT domains and will not respond to any DNS queries against zones for which they are not the authority. |

### SC-22 Architecture and Provisioning for Name / Address Resolution Service (L) (M) (H)

The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.

| SC-22 | Control Summary Information |
| --- | --- |
| Responsible Role: Azure, 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SC-22 - What is the solution and how is it implemented? |
| --- |
| **DNS:**  Office 365 DNS servers are all implemented consistently with the overall Office 365 MT architecture. Servers are deployed in a redundant, load-balanced configuration at multiple data centers. Office 365 DNS Service Team Operations regularly validates at least monthly through failover testing and exercises that any single instance is able to support the entire service if necessary.  **Bing, Delve EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT DNS servers are all implemented consistently with the overall Office 365 MT architecture. Servers are deployed in a redundant, load-balanced configuration at multiple data centers. DNS servers are either internal or external. |

### SC-23 Session Authenticity (M) (H)

The information system protects the authenticity of communications sessions.

| SC-23 | Control Summary Information |
| --- | --- |
| Responsible Role: Customer Administrator, Azure, Office 365 Security Manager, 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SC-23 - What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility:**  Government customers are responsible for having a process in place to check the validity of the Office 365 Web sites prior to signing on by reviewing the digital certificate on the site to ensure they are the Office 365 Web sites. 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.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT uses digital certificates to establish the identity of Terminal Services Gateways (TSGs) or SSH Gateways as the access point to the Office 365 MT environment. Digital certificates are used in public key cryptography (PKI) to establish the identity of a server or client for purposes of authentication. This also supports encrypted connections using TLS, which are resistant to man in the middle attacks.  All Office 365 MT servers are located within Azure data centers. Multiple physical and logical access controls in place mitigate the risk of man-in-the-middle attacks. As such, Office 365 MT has deemed it unnecessary to implement digital certificates for server-to-server connections within the environment. |

### SC-28 Protection of Information at Rest (M) (H)

The information system protects the [FedRAMP Selection: confidentiality AND integrity]] of [Assignment: organization-defined information at rest].

SC-28 Additional FedRAMP Requirements and Guidance:

Guidance: The organization supports the capability to use cryptographic mechanisms to protect information at rest.

| SC-28 | Control Summary Information |
| --- | --- |
| Responsible Role: Azure, Office 365 Security Manager | |
| Parameter SC-28:  1. confidentiality and integrity; 2. customer content | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SC-28 - What is the solution and how is it implemented? |
| --- |
| **Bing, EXO, IP, SFB:**  Office 365 MT protects the confidentiality and integrity of government customer content at rest by implementing full disk encryption. Cryptographic ciphers are employed to protect stored information using Microsoft BitLocker.  **Delve, DNS, OSI, SUE, SWE:**  These teams do not store customer content.  **SPO:**  SPO protects the confidentiality and integrity of government customer content at rest by implementing full disk encryption. Cryptographic ciphers are employed to protect stored information using Microsoft BitLocker. For more information on BitLocker, see the following TechNet article: http://technet.microsoft.com/en-us/library/hh831713.aspx. SPO further implements logical encryption of files and document content stored in Azure by using a custom encryption system, known as "per-file encryption". For more information, see:  https://technet.microsoft.com/en-us/library/dn905447.aspx  **OLM, WAC:**  OLM, and WAC protect the confidentiality and integrity of government customer content at rest using file level encryption.  **MSTeams:**  MSTeams protects the confidentiality and integrity of government customer content at rest using application-level encryption provided in Azure Storage. |

#### SC-28 (1) Control Enhancement (M)

The information system implements cryptographic mechanisms to prevent unauthorized disclosure and modification of [Assignment: organization-defined information] on [*Assignment: organization-defined information system components*]

| SC-28(1) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager | |
| Parameter SC-28(1):  1. customer content; 2. any information system components storing data defined in SC-28(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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SC-28(1) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT protects the confidentiality and integrity of government customer content at rest by implementing full disk encryption. Cryptographic ciphers are employed to protect stored information using Microsoft BitLocker. For more information on BitLocker, see the following TechNet article: http://technet.microsoft.com/en-us/library/hh831713.aspx  SPO further implements logical encryption of files and document content stored in Azure by using a custom encryption system, known as "per-file encryption". For more information, see:  https://technet.microsoft.com/en-us/library/dn905447.aspx  **OLM:**  OLM protects the confidentiality and integrity of government customer content at rest using file level encryption.  **MSTeams:**  MSTeams protects the confidentiality and integrity of government customer content at rest using application-level encryption provided in Azure Storage. |

### SC-39 Process Isolation (L) (M) (H)

The information system maintains a separate execution domain for each executing process.

| SC-39 | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SC-39 - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  All Office 365 MT servers run Windows. Windows maintains a separate execution domain for each executing process by assigning a private virtual address space to each process. See the following TechNet article for more information: http://technet.microsoft.com/en-ca/aa366785%28v=vs.90%29  For teams using Linux, a separate execution domain for each executing process is maintained by assigning a private virtual address space to each process. |

* 1. System and Information Integrity (SI)

### SI-1 System and Information Integrity Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:

A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls; and

1. Reviews and updates the current:
   1. System and information integrity policy [FedRAMP Assignment: at least every three (3) years]; and
   2. System and information integrity procedures [FedRAMP Assignment: at least at least annually].

| SI-1 | Control Summary Information |
| --- | --- |
| Responsible Role: Customer Administrator, Office 365 Security Manager, Service Engineer Operations | |
| Parameter SI-01(a)(1):  Service Engineer Operations, Program Manager, Developer, Tester, Office 365 Trust Program Manager, Office 365 Security Manager, BCM | |
| Parameter SI-01(a)(2):  Service Engineer Operations, Program Manager, Developer, Tester, Office 365 Trust Program Manager, Office 365 Security Manager, BCM | |
| Parameter SI-01(b)(1):  annually | |
| Parameter SI-01(b)(2):  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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SI-1 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Part 1:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Information Security Policy provides the overarching security guidance for Office 365 MT. This document addresses the purpose, scope, roles, responsibilities, compliance requirements, and required coordination among the various Microsoft organizations providing some level of support for the security of Office 365 MT. Policies are distributed to roles providing support for system and information integrity via SharePoint. Office 365 SOPs are distributed to roles providing support for system and information integrity via SharePoint.  **Part 2:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Standards and procedures to facilitate execution of these policies are documented in the Active Framework Controls, Office 365 Standard Operating Procedures (SOPs), and service team-specific SOPs. These standards and procedures act as adjuncts to the security policy and provide implementation level requirements and details to carry out specific operational tasks. A detailed mapping of Office 365 Standards and Procedures to each control is available. |
| Part b | **Part 1:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Information Security Policy is reviewed and updated annually.  **Part 2:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The Office 365 Standard Operating Procedures (SOPs) are reviewed and updated annually. |

### SI-2 Flaw Remediation (L) (M) (H)

The organization:

1. Identifies, reports, and corrects information system flaws;
2. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
3. Installs security-relevant software and firmware updates within [FedRAMP Assignment: thirty 30 days of release of updates] of the release of the updates; and
4. Incorporates flaw remediation into the organizational configuration management process.

| SI-2 | Control Summary Information |
| --- | --- |
| Responsible Role: Customer Administrator, Office 365 Security Manager, Service Engineer Operations | |
| Parameter SI-02(c):  30 days for high risk flaws, 90 days for moderate 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SI-2 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility:**  All customers, including government and non-government customers, are responsible for ensuring that customer users are using secure browsers and properly patched information systems to access Office 365 MT.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT identifies, reports, and corrects information system flaws through vulnerability management, incident response management, and patch/configuration management processes. The Office 365 Security Incident Response Program assists with identifying and reporting of information system flaws. Office 365 MT receives vulnerability-related data from multiple sources of information which include: Microsoft Security Resource Center (MSRC), vendor Web sites, other third-party services (e.g. Internet Security Systems) and internal/external vulnerability scanning of services. Office 365 Security will determine which updates are applicable within the Office 365 MT environment. Potential changes are tested in advance. Patching schedules are defined by Office 365 Security as follows:  • 30 days for high vulnerabilities  • 90 days for medium/moderate & low vulnerabilities  Additionally, the Office 365 PAVCteam analyzes and tests vendor-supplied software (BeyondTrust). Flaws found during testing are reported to the appropriate vendor, and vendor patches are tested and applied as they are received.  Office 365 MT inherits firmware changes from Azure, which is responsible for firmware updates to the Office 365 infrastructure. Azure has a FedRAMP IaaS P-ATO (package ID F1209051525). |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT service teams test potential software changes prior to deployment, either in a separate test environment, or by removing a server from production, making changes, testing, and returning it to production upon successful completion.  Office 365 MT inherits the testing of firmware from Azure, which is responsible for the testing of firmware prior to deployment into the Office 365 infrastructure. Azure has a FedRAMP IaaS P-ATO (package ID F1209051525). |
| Part c | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  As described in part a of this control, Office 365 MT installs security-relevant software updates within 30 days for updates associated with high risk vulnerabilities and 90 days for updates associated with medium/moderate & low risk vulnerabilities.  Office 365 MT inherits the installation of firmware from Azure, which is responsible for the installation of firmware into the Office 365 infrastructure. Azure has a FedRAMP IaaS P-ATO (package ID F1209051525).  For teams using PilotFish, firmware and software updates are managed by PilotFish. All PilotFish machines are required to receive security updates within 30 days of release and must apply OS upgrades once a month. |
| Part d | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The flaw remediation process follows the standard configuration management process, which includes testing, reviews, flaw remediation, and approvals of changes before they are installed in the production environment. The configuration management process is documented in the CM family of controls. |

#### SI-2 (2) Control Enhancement (M) (H)

The organization employs automated mechanisms [FedRAMP Assignment: at least monthly] to determine the state of information system components with regard to flaw remediation.

| SI-02(2) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager | |
| Parameter SI-02(2):  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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SI-02(2) - What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility:**  Government customers are required to employ automated mechanisms to determine the state of information system components with regard to flaw remediation on their information systems as required by their organization’s security policy  Non-Government customers of Office 365 MT inherit automated protection mechanisms from Microsoft within the environment. Non-Government customers are responsible for client-side network scans on all their endpoints in accordance with their security policy.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT utilizes BeyondTrust for vulnerability management. This tool performs periodic and on-demand scanning against the environment and determine the state of information system components with regard to flaw remediation. BeyondTrust uses the patch and vulnerability information from industry sources to scan the Office 365 MT environment. These scans are configured to run at least monthly. |

#### SI-2 (3) Control Enhancement (M) (H)

The organization:

1. Measures the time between flaw identification and flaw remediation; and
2. Establishes [Assignment: organization-defined benchmarks] for taking corrective actions.

| SI-2 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager, Office 365 Trust Program Manager | |
| Parameter SI-02(3)(b):  30 days for high risk flaws, 90 days for moderate 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SI-2 (3) - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  As part of the Office 365 MT PAVC process, the scanners produce timestamps which are kept for initial flaw detections and remediation and are used to calculate the time elapsed between the two. |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT uses the PAVC process to continuously track and correct information system flaws as detailed in RA-5. The benchmarks are to remediate high risk flaws within 30 days of discovery and moderate and low risk flaws within 90 days of discovery. |

### SI-3 Malicious Code Protection (L) (M)

The organization:

1. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code;

Updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures;

Configures malicious code protection mechanisms to:

Perform periodic scans of the information system [FedRAMP Assignment: at least weekly] and real-time scans of files from external sources at [FedRAMP Assignment: to include endpoints] as the files are downloaded, opened, or executed in accordance with organizational security policy; and

[FedRAMP Assignment: to include alerting administrator or defined security personnel] in response to malicious code detection; and

Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

| SI-3 | Control Summary Information |
| --- | --- |
| Responsible Role: Customer Administrator, Office 365 Security Manager, Service Engineer Operations | |
| Parameter SI-03(c)(1):  1. at least weekly 2. endpoint | |
| Parameter SI-03(c)(2):  block and quarantine malicious code, alert Service Engineer Operations and Office 365 Security Manager | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SI-3 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility:**  All customers, including government and non-government customers, are responsible for ensuring that customer users are using information systems running anti-malware software to access Office 365 MT.  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The use of anti-malware software is a principal mechanism for protection of Office 365 MT assets from malicious software. The software detects and prevents the introduction of computer viruses, malware, rootkits, worms, and other malicious software onto the service systems. Anti-malware software provides both preventive and detective control over malicious software. Forefront Endpoint Protection (FEP) or Microsoft Endpoint Protection (MEP) is installed as part of the initial build on all systems. ClamAV is installed on all systems for teams using Linux. Additionally, IP scans and quarantines in real time all email and email attachments both entering and leaving the system for viruses and other malware. |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Each anti-malware package tracks the version of the software and what signatures are running. The automatic download and application of signature updates at least daily from the vendor's virus definition site is centrally managed by the appropriate anti-malware tool for each service team. |
| Part c | **Part 1:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  The following functions are centrally managed by the appropriate anti-malware tool on each endpoint for each service team:  • Periodic scans of the file system (at least weekly)  • Real-time scans of files as they are downloaded, opened, or executed  Anti-malware tools detect files determined to be malicious and send alerts to Office 365 MT administrators, which triggers the incident response process.  **Part 2:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  When anti-malware tools detect malware, they block the malware and an alert is generated and sent to Office 365 MT service team personnel, Office 365 Security, and/or Azure OSSC. The receiving personnel initiate the Incident Response process. Incidents are tracked and resolved, and post mortem analysis is performed, as discussed in the Office 365 Security Incident Response Plan. |
| Part d | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  When anti-malware tools detect malware, they block the malware and an alert is generated and sent to Office 365 MT service team personnel, Office 365 Security, and/or Azure OSSC. The receiving personnel initiate the Incident Response process. Incidents are tracked and resolved, and post mortem analysis is performed, as discussed in the Office 365 Security Incident Response Plan. |

#### SI-3 (1) Control Enhancement (M) (H)

The organization centrally manages malicious code protection mechanisms.

| SI-03(1) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager, 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SI-03(1) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Forefront Endpoint Protection (FEP) or Microsoft Endpoint Protection (MEP) is installed on all systems.  ClamAV is installed on all systems for teams using Linux. The following functions are centrally managed by the appropriate anti-malware tool for each service team:  • Automatic download and application of signature updates at least daily from the vendor's virus definition site  • Periodic scans of the file system  • Automatic scans of the environment  • Alerting, cleaning, and mitigation of detected malware  • Centralized management of the anti-malware environment by Azure or Service Team Operations |

#### SI-3 (2) Control Enhancement (M) (H)

The information system automatically updates malicious code protection mechanisms.

| SI-03(2) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager, 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SI-03(2) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Automatic download and application of signature updates occurs at least daily from the vendor's virus definition site, and is centrally managed by the appropriate anti-malware tool for each service team.  For teams using PilotFish, download and application of signature updates occurs at least weekly from the vendor’s virus definition site, and is centrally managed by PilotFish. |

#### SI-3 (7) Control Enhancement (M) (H)

The information system implements nonsignature-based malicious code detection mechanisms.

| SI-03(7) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager, 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SI-03(7) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT utilizes System Center Endpoint Protection (SCEP), and the Azure Security Pack, to detect malicious code. In addition to signature-based detection mechanisms, System Center Endpoint Detection also utilizes behavior monitoring, network inspection, and heuristics in order to detect malicious code that may be missed by signature-based methods. Teams using Linux use ClamAV which utilizes heuristics in addition to signature-based detection mechanisms to detect malicious code. |

### SI-4 Information System Monitoring (L) (M) (H)

The organization:

1. Monitors the information system to detect:
   1. Attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; and

Unauthorized local, network, and remote connections;

1. Identifies unauthorized use of the information system through [Assignment: organization-defined techniques and methods];
2. Deploys monitoring devices (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization;
3. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;

Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information;

1. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and
2. Provides [Assignment: organization-defined information system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]].

SI-4 Additional FedRAMP Requirements and Guidance:

Guidance: See US-CERT Incident Response Reporting Guidelines.

| SI-4 | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager, Service Engineer Operations | |
| Parameter SI-04(a)(1):  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 monitoring objectives as described in system specific SCOM packs. | |
| Parameter SI-04(b):  automated security alerting tools and Microsoft Cosmos or Geneva | |
| Parameter SI-04(g):  1. monitoring for information specified by Office 365 Security Team; 2. Office 365 Security Manager; 3. daily and 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SI-4 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Part 1:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Service teams have deployed active monitoring solutions that generate all real-time alerts and audit logs from both SCOM and the uploader service. All the service team-specific monitoring requirements beyond the base set defined in Office 365 Security Auditing SOP for Office 365 MT are integrated into a SCOM pack. In addition, service teams upload their logs to a repository service, where they are aggregated and processed. The uploader service generates reports using automated security alerting tools. Office 365 Security assists in identifying normal usage of the system and deviations from that normal range. Office 365 Security examines records to confirm that the system is functioning in an optimal, resilient, and secure state. Unusual activity is flagged for further review. Any log event that indicates a potential security violation must be immediately brought to the attention of Office 365 Security.  Teams using PilotFish use K9, a tool that collects security logs and performs real-time analysis, as well as archiving them to a repository service for forensic analysis. Unusual activity will generate alerts and the PilotFish team coordinates with the appropriate service team for any required follow-ups or investigations. Service teams will work with the Office 365 SIR team to address all security incidents.  **Part 2:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Local connections are disallowed by policy within Office 365 MT. No personnel have local access. Azure performs network monitoring and detection of unauthorized connections in accordance with their security policy. Remote authentication failures are logged and stored within a repository service. For further information, please see AC-17 and AC-7. |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Audit logs are uploaded to a repository service and reports are generated using automated security alerting tools. Office 365 Security assists in identifying normal usage of the system and deviations from that normal range. The automated security alerting tools use heuristics to identify unauthorized use of the operating system. Unusual activity is flagged for further review. Any log event that indicates a potential security violation must be immediately brought to the attention of Office 365 Security.  For teams using PilotFish, audit logs are uploaded to a repository service and reports are generated using PilotFish/K-9. PilotFish/K-9 assists in identifying normal usage of the system and deviations from that normal range. PilotFish/K-9 uses heuristics to identify unauthorized use of the operating system. Unusual activity is flagged for further review. Any log event that indicates a potential security violation must be immediately brought to the attention of Office 365 Security. |
| Part c | **Part 1:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  All servers act as monitoring devices and are configured to log all security-relevant events. Office 365 MT monitors all hosts in the environment. Suspicious events generate alarms and notifications to service team staff and appropriate contingent staff. Logs are aggregated in a repository service and reports are generated using automated security alerting tools.  For teams using PilotFish, all servers act as monitoring devices and are configured to log all security-relevant events. Office 365 MT monitors all hosts in the environment. Suspicious events generate alarms and notifications to service team staff and appropriate contingent staff. Logs are aggregated in a repository service and reports are generated using PilotFish/K-9.  **Part 2:**  **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  All servers are configured to log all exceptions and security-relevant events. Office 365 MT has determined that there is no need for ad-hoc deployment of monitoring devices as documented in "Ad-hoc Monitoring Devices Decision Log (SI-4)". |
| Part d | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  All servers upload logs to a repository service for aggregation and analysis. Access to the repository service is restricted as specified in the AU family of controls, specifically AU-9. |
| Part e | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 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. Servers are configured to increase logging parameters in response to an indication of increased risk, and automated security alerting tool heuristics are tailored to look for specific threats based on the nature of the risk to organizational operations and assets. |
| Part f | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 Security, in consultation with Corporate External Legal Affairs (CELA), has defined a set of log events and alerts that meet federal 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 Office 365 MT services. To fully comply with applicable regulations, the service teams follow defined requirements for event collection and notification processes. These requirements are contained in both the Office 365 Security or PilotFish/K-9 Onboarding documents. |
| Part g | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  All servers upload logs to a repository service for aggregation and analysis. Reports are generated from this data using automated security alerting tools as described AU-6 and AU-7. These reports are available daily and as needed.  For teams using PilotFish, all servers upload logs to a repository service for aggregation and analysis. Reports are generated from this data using PilotFish/K-9 as described AU-6 and AU-7. These reports are available daily and as needed. |

#### SI-4 (1) Control Enhancement (M) (H)

The organization connects and configures individual intrusion detection tools into an information system-wide intrusion detection system.

| SI-04(1) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager, 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SI-04(1) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  All servers upload logs to a repository service for aggregation and analysis. Consolidated reports are generated from this data using the automated security alerting tools as described AU-6 and AU-7, and cover system-wide intrusion detections.  For teams using PilotFish, audit logs are uploaded to a repository service for aggregation and analysis. Reports are generated from this data using PilotFish/K-9 as described AU-6 and AU-7. These reports are available daily and as needed. |

#### SI-4 (2) Control Enhancement (M) (H)

The organization employs automated tools to support near real-time analysis of events.

| SI-04(2) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager, 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SI-04(2) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Service teams operate active monitoring systems that generate automated real-time alerts and audit logs from both SCOM and the uploader service. These automated tools perform analysis and trigger emails to Service Team Engineering groups when a specified threshold has been reached or event has occurred. Upon receipt, Service Team Engineering personnel uses a ticketing tool and creates a bug to analyze and track the issue and follow incident response procedures.  Teams using PilotFish use K9, a tool that collects security logs and performs real-time analysis. Unusual activity generates alerts, and the PilotFish team coordinates with the appropriate service team for any required follow-ups or investigations. Service teams will work with the Office 365 SIR team to address all security incidents. |

#### SI-4 (4) Control Enhancement (M) (H)

The information system monitors inbound and outbound communications traffic [FedRAMP Assignment: continuously] for unusual or unauthorized activities or conditions.

| SI-04(4) | Control Summary Information |
| --- | --- |
| Responsible Role: Azure, Office 365 Security Manager, Service Engineer Operations | |
| Parameter SI-04(4):  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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SI-04(4) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Azure monitors for unusual traffic patterns using OneDDOS. In addition, service teams monitor for denial of service attacks by monitoring the following key health metrics: CPU usage, network connections, disk input/output operations per second (IOPS), and disk space usage. Office 365 MT service teams also monitor and review web server (e.g. IIS) logs and other application logs (as applicable) for unusual or unauthorized activities or conditions. Any unapproved connections detected through auditing or alerting will be triaged using security incident response processes. |

#### SI-4 (5) Control Enhancement (M) (H)

The information system alerts [Assignment: organization-defined personnel or roles] when the following indications of compromise or potential compromise occur: [Assignment: organization-defined compromise indicators].

SI-4(5) Additional FedRAMP Requirements and Guidance:

Guidance: In accordance with the incident response plan.

| SI-04(5) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager, Service Engineer Operations | |
| Parameter SI-04(5):  1. personnel defined in the Incident Response plan; 2. criteria defined in the Incident Response plan | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SI-04(5) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 Security has defined requirements for active monitoring. Service teams configure active monitoring tools in accordance with these requirements. Active monitoring tools include System Center Operations Manager (SCOM) and the automated security alerting tools, which are configured to provide real time alerts to Service Team Operations personnel in situations that require immediate action.  For teams using PilotFish use K-9 which is configured to provide real time alerts to Service Team Operations personnel in situations that require immediate action. The list of events being monitored is stored on each respective team’s SharePoint site. |

#### SI-4 (14) Control Enhancement (M) (H)

The organization employs a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information system.

| SI-04(14) | Control Summary Information |
| --- | --- |
| Responsible Role: Azure, Office 365 Security Manager, 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SI-04(14) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Azure regularly monitors for rogue wireless signals on a quarterly basis as discussed in AC-18. |

#### SI-4 (16) Control Enhancement (M) (H)

The organization correlates information from monitoring tools employed throughout the information system.

| SI-04(16) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager, 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SI-04(16) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  All servers upload logs to a for aggregation and analysis. Reports are generated from this data using automated security alerting tools as described AU-6 and AU-7, and cover system-wide intrusion detections.  For teams using PilotFish, all servers upload logs to a repository service for aggregation and analysis. Reports are generated from this data using K-9 as described in AU-6 and AU-7, and cover system-wide intrusion detections. |

#### SI-4 (23) Control Enhancement (M) (H)

The organization implements [Assignment: organization-defined host-based monitoring mechanisms] at [Assignment: organization-defined information system components].

| SI-04(23) | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager, Service Engineer Operations | |
| Parameter SI-04(23):  1. Windows Event Logging; 2. all hosts | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SI-04(23) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  All Windows hosts within Office 365 MT have Windows Event Logging enabled. If this functionality is turned off or unsuccessful, an alert will be generated through the uploader service and automated security alerting tools and the alert will be investigated as a security incident. For teams using PilotFish, an alert will be generated through the uploader service and K-9, and the alert will be investigated as a security incident.  Linux hosts within Office 365 MT use AuditD or the Azure Monitoring and Diagnostics System (MDS) to capture logs and send them to an audit log repository service. If this functionality is turned off or unsuccessful, an alert will be generated and investigated as a security incident. |

### SI-5 Security Alerts & Advisories (L) (M) (H)

The organization:

1. Receives information system security alerts, advisories, and directives from [FedRAMP Assignment: to include US-CERT] on an ongoing basis;
2. Generates internal security alerts, advisories, and directives as deemed necessary;
3. Disseminates security alerts, advisories, and directives to [FedRAMP Assignment: to include system security personnel and administrators with configuration/patch-management responsibilities]; and
4. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.

| SI-5 | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager, Service Engineer Operations | |
| Parameter SI-05(a):  the Microsoft Security Bulletin Advance Notice, through government sources including US-CERT, and directly from vendors | |
| Parameter SI-05(c):  Service Engineer Operations and Office 365 Security Manager | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SI-5 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT service teams receive information system security alerts, advisories, and directives from the Office 365 Security and Azure teams. These teams are responsible for receiving alerts on an ongoing basis from designated external organizations (including US-CERT) and pushing them to the Office 365 MT service teams. |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Internal alerts are generated from tools within Office 365 MT such as antivirus, OneDDOS, and logging/monitoring tools.  Azure also disseminates alerts received from vendor Web sites, other third-party services (Internet Security Systems, US-CERT advisories and alerts) and shares this information with throughout the organization. Additionally, Microsoft publishes bulletins through the Microsoft Security Response Center (MSRC) which include specific information relevant to security updates being released. In general, only Critical and Important bulletins are reviewed by Office 365 Security. The Office 365 Security team also addresses notifications and disseminates security alerts (e.g. email, RSS feeds) received directly from external organizations (US-CERT) other than the Services Operation Center or Microsoft Support. |
| Part c | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Security alerts, advisories, and directives are disseminated to Office 365 MT Service Team Operations and Security Manager personnel and FedRAMP (including FedRAMP ISSO). |
| Part d | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  When security updates are identified from the above information sources, they are initially reviewed by Office 365 MT Service Team Engineering personnel. Qualified updates are pushed through monthly/emergency triage meetings to appropriate service groups who are responsible for patching servers appropriately and verify that servers are operational. Security remediation will be implemented as follows:  • Remediation for High Risk vulnerabilities will be implemented within 30 days of the vulnerability mitigation being released by the vendor.  • Remediation for Medium Risk vulnerabilities will be implemented within 90 days of vulnerability the vulnerability mitigation being released by the vendor.  • Low Risk scan results are risk reviewed by Office 365 Security. Many Low Risk scan results are determined by Office 365 Security to pose no risk to Office 365 MT. In this case, an exception is filed and the result is not remediated. If the result is determined to pose any risk to Office 365 MT the result is escalated to Medium Risk and remediated according to the Medium Risk timeframe.  In the event where patching during the timeframe is infeasible, service groups may request exceptions, which are very limited and reviewed on a case-by-case basis. Exceptions and risks identified during the course of vulnerability remediation are tracked in Archer for stakeholder and Office 365 Security review. Office 365 Security also verifies degree of compliance using vulnerability scanners deployed in Office 365 MT. |

### SI-6 Security Functionality Verification (M) (H)

The information system:

1. Verifies the correct operation of [Assignment: organization-defined security functions];
2. Performs this verification [FedRAMP Assignment: to include upon system startup and/or restart at least monthly];
3. Notifies [FedRAMP Assignment: to include system administrators and security personnel] of failed security verification tests; and
4. [Selection (one or more): shuts the information system down; restarts the information system; [FedRAMP Assignment: to include notification of system administrators and security personnel] when anomalies are discovered.

| SI-6 | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager, Service Engineer Operations | |
| Parameter SI-06(a):  functions verified by WRP | |
| Parameter SI-06(b):  upon startup and restart | |
| Parameter SI-06(c):  Office 365 Security Manager | |
| Parameter SI-06(d):  Restarts the information system or security function | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SI-6 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT service teams using Windows run Windows Resource Protection (WRP), which verifies the correct operation of core Windows Server security functions at boot. WRP is a built-in part of the Windows operating system. Linux systems integrate these checks into Cassandra for file system errors. Monitoring is configured to alert when these tools report errors; monitoring alerts result in the appropriate incident response process being followed. For more information on these tools, see the following link: http://msdn.microsoft.com/en-us/library/windows/desktop/aa382503(v=vs.85).aspx. All servers are rebooted at least monthly to support patching, which also provides a check to prevent malicious changes introduced during operation.  Office 365 MT has determined that solutions more comprehensive than WRP pose unacceptable risks to system availability. A complete discussion of these risks and the mitigating controls in place are documented in CM-7(2) Decision Log.  Linux hosts use Samhain or the FSCK utility to monitor changes to files or directories. |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  All Office 365 MT service teams run Windows Resource Protection (WRP), which verifies the correct operation of core Windows Server security functions at boot. WRP is a built-in part of the Windows operating system. Linux systems integrate these checks into Cassandra for file system errors. Monitoring is configured to alert when these tools report errors; monitoring alerts result in the appropriate incident response process being followed. For more information on these tools, see the following link: http://msdn.microsoft.com/en-us/library/windows/desktop/aa382503(v=vs.85).aspx. All servers are rebooted at least monthly to support patching, which also provides a check to prevent malicious changes introduced during operation.  Linux hosts use Samhain or the FSCK utility to monitor changes to files or directories. |
| Part c | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  For Windows hosts, WRP replaces files that fail integrity checks automatically. Linux hosts use Samhain or the FSCK utility to monitor changes to files or directories. Office 365 MT has determined that solutions to fully meet this control pose unacceptable risks to system availability. A complete discussion of these risks and the mitigating controls in place are documented in CM-7(2) Decision Log.monitors what files and/or directories have been changed, deleted, or added. |
| Part d | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  For Windows hosts, WRP replaces files that fail integrity checks automatically. Linux hosts use Samhain or the FSCK utility to monitor changes to files or directories. Office 365 MT has determined that solutions to fully meet this control pose unacceptable risks to system availability. A complete discussion of these risks and the mitigating controls in place are documented in CM-7(2) Decision Log. |

### SI-7 Software & Information Integrity (M) (H)

The organization employs integrity verification tools to detect unauthorized changes to [Assignment: organization-defined software, firmware, and information].

| SI-07 | Control Summary Information |
| --- | --- |
| Responsible Role: Office 365 Security Manager, Service Engineer Operations | |
| Parameter SI-07:  files protected by WRP | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SI-07 - What is the solution and how is it implemented? |
| --- |
| **Bing:**  Integrity verification mechanisms are inherited from PilotFish. Integrity checks are performed against PilotFish signatures. If system integrity is compromised, PilotFish will revert back to a healthy image. Firmware verification is inherited from Azure. Teams using Linux use the File System Consistency Check (FSCK) utility for validation and recovery of core files.  **DNS, IP, SFB, SPO, SWE, WAC:**  The Microsoft Windows operating systems on Office 365 MT information systems provide file integrity validation, protection, and recovery of core system files that are installed as a part of the original installation or authorized system updates, detecting unauthorized changes.  Teams using Azure inherit firmware verification from Azure. Teams using Azure inherit firmware verification from Azure.  Office 365 MT has determined that solutions to fully meet this control pose unacceptable risks to system availability. A complete discussion of these risks and the mitigating controls in place are documented in CM-7(2) Decision Log. This decision log was reviewed as part of the 2015 FedRAMP audit and documented as an operational requirement in the 2015 FedRAMP SAR.  **Delve, EXO:**  The Microsoft Windows operating systems on Office 365 MT information systems provide file integrity validation, protection, and recovery of core system files that are installed as a part of the original installation or authorized system updates, detecting unauthorized changes.  For Delve and EXO, AppLocker detects unauthorized changes to software and information.  **MSTeams, OSI, SUE:**  Integrity verification mechanisms are inherited from Windows Azure, which has a FedRAMP IaaS/PaaS P-ATO (package ID F1209051525), and is secured via an Interconnection Security Agreement; Office 365 MT ISA with Windows Azure.  **OLM:**  OLM uses a tool called Samhain for file integrity checking and log file monitoring/analysis; Samhain monitors what files and/or directories have been changed, deleted, or added. |

#### SI-7 (1) Control Enhancement (M) (H)

The information system performs an integrity check of [Assignment: organization-defined software, firmware, and information] [FedRAMP Selection (one or more): at startup; at [FedRAMP Assignment: to include security-relevant events]; [FedRAMP Assignment: at least monthly]].

| SI-07(1) | Control Summary Information |
| --- | --- |
| Responsible Role: Azure, Office 365 Security Manager, Office 365 Trust Program Manager | |
| Parameter SI-07(1):  1. files protected by WRP; 2. at startup; 3. 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SI-07(1) - What is the solution and how is it implemented? |
| --- |
| **Bing:**  Integrity verification mechanisms are inherited from PilotFish. Integrity checks are performed against PilotFish signatures. If system integrity is compromised, PilotFish will revert back to a healthy image. Firmware verification is inherited from Azure. Teams using Linux use the File System Consistency Check (FSCK) utility for validation and recovery of core files.  **DNS, IP, SFB, SPO, SWE, WAC:**  Office 365 MT has determined that solutions to fully meet this control pose unacceptable risks to system availability. A complete discussion of these risks and the mitigating controls in place are documented in CM-7(2) Decision Log. This decision log was reviewed as part of the 2015 FedRAMP audit and documented as an operational requirement in the 2015 FedRAMP SAR.  **Delve, EXO:**  AppLocker has been implemented to assess the integrity of the system.  **MSTeams, OSI, SUE:**  Integrity verification mechanisms are inherited from Windows Azure, which has a FedRAMP IaaS/PaaS P-ATO (package ID F1209051525), and is secured via an Interconnection Security Agreement; Office 365 MT ISA with Windows Azure.  **OLM:**  OLM uses a tool called Samhain for file integrity checking and log file monitoring/analysis; Samhain monitors what files and/or directories have been changed, deleted, or added. |

#### SI-7 (7) Control Enhancement (M) (H)

The organization incorporates the detection of unauthorized [Assignment: organization-defined security-relevant changes to the information system] into the organizational incident response capability.

| SI-07(7) | Control Summary Information |
| --- | --- |
| Responsible Role: Azure, Office 365 Security Manager, Office 365 Trust Program Manager | |
| Parameter SI-07(7):  files protected by WRP | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SI-07(7) - What is the solution and how is it implemented? |
| --- |
| **DNS, IP, OLM, SFB, SPO, SWE, WAC:**  Office 365 MT has determined that solutions to fully meet this control pose unacceptable risks to system availability. A complete discussion of these risks and the mitigating controls in place are documented in CM-7(2) Decision Log.  **Delve, EXO:**  AppLocker has been implemented to assess the integrity of the system. AppLocker generates alerts to Service Team Operations personnel, who initiate the incident response process as needed.  **Bing, MSTeams, OSI, SUE:**  Integrity verification mechanisms are inherited from Azure, which has a FedRAMP IaaS/PaaS P-ATO (package ID F1209051525), and is secured via an Interconnection Security Agreement Office 365 MT ISA with Azure. |

### SI-8 Spam Protection (M) (H)

The organization:

1. Employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages; and
2. Updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policies and procedures.

| SI-8 | Control Summary Information |
| --- | --- |
| Responsible Role: 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SI-8 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  IP provides spam protection mechanisms for all Office 365 MT customers for external incoming email. This filtering solution provides enterprise-class reliability for messaging security and management, and protects against spam and malware. All inbound Internet email traffic is routed through IP, where each message is evaluated against predefined rules.  The IP system builds spam lists internally and consumes spam lists from Spamhaus (http://www.spamhaus.org/) to prevent known spam offenders from getting messages through the system and into customer mailboxes. All external incoming email must pass through the spam filtering system. |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Internal spam lists are updated by automated processes on an ongoing basis. Externally-provided spam lists are updated whenever updates are available from Spamhaus, which is checked multiple times per day. |

#### SI-8 (1) Control Enhancement (M) (H)

The organization centrally manages spam protection mechanisms.

| SI-08(1) | Control Summary Information |
| --- | --- |
| Responsible Role: 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SI-08(1) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  IP provides a centrally managed spam protection mechanism for all Office 365 MT customers for external incoming email. This filtering solution protects against spam and malware. All inbound Internet email traffic is routed through IP, where each message is evaluated against predefined rules. |

#### SI-8 (2) Control Enhancement (M) (H)

The organization automatically updates spam protection mechanisms.

| SI-08(2) | Control Summary Information |
| --- | --- |
| Responsible Role: 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SI-08(2) - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Internal spam lists are updated by spam analysts and automated processes on an ongoing basis. Externally-provided spam lists are updated whenever updates are available from Spamhaus, which is checked multiple times per day. |

### SI-10 Information Input Validation (M) (H)

The information system checks the validity of [Assignment: organization-defined information inputs].

| SI-10 | Control Summary Information |
| --- | --- |
| Responsible Role: Developer, Program Manager, Tester | |
| 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SI-10 - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT follows system development methodology and security guidelines described in the common Online Services Secure Coding Procedure. The process addresses requirements around input data validation within applications. Office 365 MT has implemented information validation through checking of data inputs.  Thorough code reviews and testing are completed during the Verification Phase prior to software being put into a production environment. The code reviews and testing check among others for cases of SQL injection, format string vulnerabilities, XSS, integer arithmetic, command injection, and buffer overflow vulnerabilities.  Applications within Office 365 MT have the capability to use drop down menus for granular control configuration, allowing selections from a predefined set of permissible actions and basic edit checks on modifiable fields to ensure accuracy, completeness, validity, and authenticity of input information. For example, basic validation checks on fields used to capture file names, search criteria, etc.  Office 365 MT host servers require that information that is input to be in the form of machine-recognizable language in specific syntax or format, or the information will be rejected.  In addition, Office 365 DNS leverages the intrusion detection/prevention service provided by Azure, OneDDOS, to validate incoming DNS requests. OneDDOS provides the ability to identify malformed DNS requests and will alert and respond to malicious requests. |

### SI-11 Error Handling (M) (H)

The information system:

1. Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries; and
2. Reveals error messages only to [Assignment: organization-defined personnel or roles].

| SI-11 | Control Summary Information |
| --- | --- |
| Responsible Role: Developer, Program Manager, Tester | |
| Parameter SI-11(b):  Service Engineer Operations, Office 365 Security Manager | |
| Implementation Status (check all that apply):  Implemented  Partially Implemented  Planned  Alternative Implementation  Not Applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SI-11 - What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT applications, operating systems, and platforms identify error conditions, generate user-friendly error messages with correlation IDs, and provide information necessary for corrective actions without revealing sensitive information and log details within operating system and application logs which are only accessible by authorized service personnel and Office 365 MT customer administrators. |
| Part b | **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  See SI-11(a) |

### SI-12 Information Output Handling and Retention (L) (M) (H)

The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

| SI-12 | Control Summary Information |
| --- | --- |
| Responsible Role: Customer Administrator, Program Manager, 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SI-12 - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Office 365 MT owned assets are retained as appropriate based on retention requirements set by Corporate Records Management and an asset’s classification, or based on contractual requirements. Microsoft guarantees retention of tenant data for 30 days after termination and all information is permanently deleted 90 days after termination of service. The classification of assets is included in the Office 365 MT asset inventory. Refer to Corporate Records Management’s Microsoft Documentation Retention Policy (available for onsite review at http://lcaweb/policies/EmployeeConduct/retention/Pages/DocumentRetentionPolicy.aspx), which describes which Microsoft documents must be kept and for how long.  Additionally, Office 365 MT has a comprehensive framework to comply with FedRAMP, SOC I, SOC II, HIPAA, ISO27001, EUMC, and other regulations as necessary. As part of this framework, Office 365 maintains ongoing continuous monitoring programs to assure compliance in post-production deployments. |

### SI-16 Memory Protection (M) (H)

The information system implements [Assignment: organization-defined fail-safe procedures] to protect its memory from unauthorized code execution.

| SI-16 | Control Summary Information |
| --- | --- |
| Responsible Role: Program Manager, Service Engineer Operations | |
| 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 Provisional Authority to Operate (P-ATO) for Azure (F1209051525)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Azure Government (F1603087869)  Not Applicable | |

| SI-16 - What is the solution and how is it implemented? |
| --- |
| **Bing, Delve, DNS, EXO, IP, MSTeams, OLM, OSI, SFB, SPO, SUE, SWE, WAC:**  Windows has 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, Microsoft requires secure coding practices including explicit consideration for safe memory handling requirements.  See the following TechNet articles for more information about these protections:  • http://technet.microsoft.com/en-us/library/aa366553.aspx  • http://technet.microsoft.com/en-us/library/bb457155.aspx  • http://technet.microsoft.com/en-us/library/cc771361%28v=WS.10%29.aspx  Linux uses Address Space Layout Randomization to prevent code execution in restricted memory locations. |

1. Acronyms

The master list of FedRAMP acronym and glossary definitions for all FedRAMP templates is available on the FedRAMP website Documents page under Program Overview Documents.

Please send suggestions about corrections, additions, or deletions to info@fedramp.gov.

SYSTEMS SECURITY PLAN ATTACHMENTS

1. Attachments

A recommended attachment file naming convention is provided in Table 15‑1. Attachment File Naming Convention below. Use this to generate names for the attachments. Make only the following additions/changes to Table 15.1:

* The first item, Information Security Policies and Procedures (ISPP), may be fulfilled by multiple documents. If that is the case, add lines to Table 15‑1 Attachment File Naming Convention to differentiate between them using the “ISP” portion of the File Name. Example Office 365 MT A1 ISPP xx v1.0. Delete the “xx” if there is only one document.
* Enter the file extension for each attachment.
* Do not change the Version Number in the File Name in Table 15‑1 Attachment File Naming Convention. (Information System Abbreviation, attachment number, document abbreviation, version number)

Table 15‑1 Attachment File Naming Convention

|  |  |  |
| --- | --- | --- |
| Attachment | File Name | File Extension |
| Information Security Policies and Procedures | Office 365 MT A1 ISPP xx v1.0 | . |
| User Guide | Office 365 MT A2 UG v1.0 | . |
| E-Authentication Worksheet | Included in Section 15 | . |
| PTA | Included in Section 15 | . |
| PIA If needed) | Office 365 MT A4 PIA v1.0 | . |
| Rules of Behavior | Office 365 MT A5 ROB v1.0 | . |
| Information System Contingency Plan | Office 365 MT A6 ISCP v1.0 | . |
| Configuration Management Plan | Office 365 MT A7 CMP v1.0 | . |
| Incident Response Plan | Office 365 MT A8 IRP v1.0 | . |
| CIS Summary Report | Office 365 MT A9 CIS Report v1.0 | . |
| CIS Worksheet | Office 365 MT A9 CIS WSv1.0 | . |
| FIPS 199 | Included in Section 15 | . |
| Inventory | Office 365 MT A13 INV v1.0 | . |
| Ports & Protocols | Office 365 MT A14 PP v1.0 | . |

ATTACHMENT 1 - Information Security Policies and Procedures

All Authorization Packages must include an Information Security Policies and Procedures attachment, which will be reviewed for quality. This attachment has been provided separately to 3PAO.

ATTACHMENT 2 - User Guide

All Authorization Packages must include a User Guide attachment, which will be reviewed for quality. This attachment has been provided separately to 3PAO.

ATTACHMENT 3 – e-Authentication Worksheet

The E-Authentication section explains the objective for selecting the appropriate e-Authentication level for the candidate system. Guidance on selecting the system authentication technology solution is available in NIST SP 800-63, Revision 1, Electronic Authentication Guideline. This attachment has been provided separately to 3PAO.

### Introduction and Purpose

This document provides guidance on electronic authentication (E-Authentication, which is the process of establishing confidence in user identities electronically presented to an information system. Authentication focuses on confirming a person’s identity, based on the reliability of his or her credential. Office of Management and Budget (OMB) Memorandum M-04-04, E-Authentication Guidance for Federal Agencies requires federal information system owners determine the system’s electronic authentication (E-Authentication) requirements to minimize the potential impact of authentication errors and misuse of credentials.

OMB Memorandum M-04-04 can be found at the following URL: OMB M-04-04.pdf

### Information System Name/Title

This E-Authentication Plan provides an overview of the security requirements for the Office 365 MultiTenant Cloud (Office 365 MT) in accordance with OMB Memo M-04-04.

Table ‑ Information System Name and Title

| Unique Identifier | Information System Name | Information System Abbreviation |
| --- | --- | --- |
| F1209231600 | Office 365 MultiTenant | Office 365 MT |

### E-Authentication Level Definitions

The OMB memo defines four authentication levels to categorize a federal information system’s E-Authentication posture. The OMB Memo defines the four E-Authentication levels as:

* Level 1: Little or no confidence in the asserted identity’s validity
* Level 2: Some confidence in the asserted identity’s validity
* Level 3: High confidence in the asserted identity’s validity
* Level 4: Very high confidence in the asserted identity’s validity

Selecting the appropriate E-Authentication level for a system enables the system owner to determine the right system authentication technology solution for the selected E-Authentication level. Guidance on selecting the system authentication technology solution is available in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63, Revision 2, Electronic Authentication Guideline.

NIST SP 800-63, Revision 2 can be found at the following URL: SP 800-63-2

### Review Maximum Potential Impact Levels

Microsoft Corporation has assessed the potential risk from E-Authentication errors, or E-Authentication misuse, related to a user’s asserted identity. Microsoft Corporation has taken into consideration the potential for harm (impact) and the likelihood of the occurrence of the harm and has identified an impact profile as found in Table 15‑3 Potential Impacts for Assurance Levels.

Assurance is defined as 1) the degree of confidence in the vetting process used to establish the identity of the individual to whom the credential was issued, and 2) the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued.

Table 15‑3 Potential Impacts for Assurance Levels

|  | Assurance Level Impact Profile | | | |
| --- | --- | --- | --- | --- |
| Potential Impact Categories | 1 | 2 | 3 | 4 |
| Inconvenience, distress or damage to standing or reputation | Low | Mod | Mod | High |
| Financial loss or agency liability | Low | Mod | Mod | High |
| Harm to agency programs or public interests | N/A | Low | Mod | High |
| Unauthorized release of sensitive information | N/A | Low | Mod | High |
| Personal Safety | N/A | N/A | Low | Mod, High |
| Civil or criminal violations | N/A | Low | Mod | High |

### E-Authentication Level Selection

The Microsoft Corporation has identified that they support the E-Authentication Level that has been selected for the Information System Name; as noted in Table 15‑4 E-Authentication Level. The selected E-Authentication Level indicated is supported for federal agency consumers of the cloud service offering. Implementation details of the E-Authentication mechanisms are provided in the System Security Plan under control IA-2

Table 15‑4 E-Authentication Level

| E-Authentication Level | Maximum Impact Profile | Selection |
| --- | --- | --- |
| Level 1: no identity proofing requirement | Low | ☐ |
| Level 2: single factor remote authentication | Low | ☐ |
| Level 3: multifactor remote authentication | Moderate | ☒ |
| Level 4: multifactor remote authentication; hard crypto tokens | High | ☐ |

ATTACHMENT 4 – PTA / PIA

All Authorization Packages must include a Privacy Threshold Analysis (PTA) and if necessary, the Privacy Impact Assessment (PIA) attachment, which will be reviewed for quality. This attachment has been provided separately to 3PAO.

The PTA is included in this section, and the PIA Template can be found on the following FedRAMP website page: [Templates](https://www.fedramp.gov/resources/templates-2016/).

The PTA and PIA Template includes a summary of laws, regulations and guidance related to privacy issues in ATTACHMENT 12 – FedRAMP Laws and Regulations.

### Privacy Overview and Point of Contact (POC)

The Table 15‑5 - Information System Name; Privacy POC individual is identified as the Information System Name; Privacy Officer and POC for privacy at Microsoft Corporation.

Table 15‑5 - Information System Name; Privacy POC

| Name |  |
| --- | --- |
| Title |  |
| CSP / Organization |  |
| Address |  |
| Phone Number |  |
| Email Address |  |

#### Applicable Laws and Regulations

The FedRAMP Laws and Regulations may be found on: [www.fedramp.gov](http://www.fedramp.gov) Templates. A summary of FedRAMP Laws and Regulations is included in the System Security Plan (SSP) ATTACHMENT 12 – FedRAMP Laws and Regulations.

Table 12‑1 Office 365 MultiTenant Cloud Laws and Regulations include additional laws and regulations that are specific to Office 365 Government Community Cloud. These will include laws and regulations from the Federal Information Security Management Act (FISMA), Office of Management and Budget (OMB) circulars, Public Law (PL), United States Code (USC), and Homeland Security Presidential Directives (HSPD).

Table 15‑6 Office 365 MultiTenant Cloud Laws and Regulations

| Identification Number | Title | Date | Link |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |

#### Applicable Standards and Guidance

The FedRAMP Standards and Guidance may be found on: [www.fedramp.gov](http://www.fedramp.gov) Templates. The FedRAMP Standards and Guidance is included in the System Security Plan (SSP) ATTACHMENT 12 – FedRAMP Laws and Regulations. For more information, see the Program Documents Overview section of the FedRAMP website.

Table 12‑2 Office 365 MultiTenant Cloud Standards and Guidance includes any additional standards and guidance that are specific to Office 365 MultiTenant Cloud. These will include standards and guidance from Federal Information Processing Standard (FIPS) and National Institute of Standards and Technology (NIST) Special Publications (SP).

Table 15‑7 Office 365 MultiTenant Cloud Standards and Guidance

| Identification Number | Title | Date | Link |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |

#### Personally Identifiable Information (PII)

Personally Identifiable Information (PII) as defined in OMB Memorandum M-07-16 refers to information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. Information that could be tied to more than one person (date of birth) is not considered PII unless it is made available with other types of information that together could render both values as PII (for example, date of birth and street address). A non-exhaustive list of examples of types of PII includes:

* Social Security numbers
* Passport numbers
* Driver’s license numbers
* Biometric information
* DNA information
* Bank account numbers

PII does not refer to business information or government information that cannot be traced back to an individual person.

### Privacy Threshold Analysis

Microsoft Corporation performs a Privacy Threshold Analysis annually to determine if PII is collected by any of the Office 365 MultiTenant (Office 365 MT) components. If PII is discovered, a Privacy Impact Assessment is performed. The Privacy Impact Assessment template used by Microsoft Corporation can be found in Section 3. This section constitutes the Privacy Threshold Analysis and findings.

#### Qualifying Questions

|  |  |
| --- | --- |
| Select One | 1. Does the ISA collect, maintain, or share PII in any identifiable form?   Yes |
| Select One | 1. Does the ISA collect, maintain, or share PII information from or about the public?   No |
| Select One | 1. Has a Privacy Impact Assessment ever been performed for the ISA?   Yes |
| Select One | 1. Is there a Privacy Act System of Records Notice (SORN) for this ISA system?  If yes; the SORN identifier and name is: Enter SORN ID/Name.   No |

#### If answers to Questions 1-4 are all “No” then a Privacy Impact Assessment may be omitted. If any of the answers to Question 1-4 are “Yes” then complete a Privacy Impact Assessment.Designation

Check one.

|  |  |
| --- | --- |
| ✔ | A Privacy Sensitive System |
| ☐ | Not a Privacy Sensitive System (in its current version) |

The Privacy Impact Assessment Template can be found on the following FedRAMP website page:

[Templates](https://www.fedramp.gov/resources/templates-2016/).

ATTACHMENT 5 - Rules of Behavior

All Authorization Packages must include a Rules of Behavior (RoB) attachment, which will be reviewed for quality. This attachment has been provided separately to 3PAO.

The RoB describes controls associated with user responsibilities and certain expectations of behavior for following security policies, standards and procedures. Security control PL-4 requires a CSP to implement rules of behavior.

The Rules of Behavior Template can be found on the following FedRAMP website page: [Templates](https://www.fedramp.gov/resources/templates-2016/).

The Template provides two example sets of rules of behavior: one for Internal Users and one for External Users. The CSP should modify each of these two sets to define the rules of behavior necessary to secure their system.

ATTACHMENT 6 – Information System Contingency Plan

All Authorization Packages must include an Information System Contingency Plan attachment, which will be reviewed for quality. This attachment has been provided separately to 3PAO.

The Information System Contingency Plan Template can be found on the following FedRAMP website page: [Templates](https://www.fedramp.gov/resources/templates-2016/).

The Information System Contingency Plan Template is provided for CSPs, 3PAOs, government contractors working on FedRAMP projects, government employees working on FedRAMP projects and any outside organizations that want to make use of the FedRAMP Contingency Planning process.

ATTACHMENT 7 - Configuration Management Plan

All Authorization Packages must include a Configuration Management Plan attachment, which will be reviewed for quality. This attachment has been provided separately to 3PAO.

ATTACHMENT 8 - Incident Response Plan

All Authorization Packages must include an Incident Response Plan attachment, which will be reviewed for quality. This attachment has been provided separately to 3PAO.

ATTACHMENT 9 - CIS Report and Worksheet

All Authorization Packages must include Control Implementation Summary (CIS) Report and Worksheet attachments, which will be reviewed for quality. This attachment has been provided separately to 3PAO.

Templates for both can be found on the following FedRAMP website page: Templates.

The Report Template has a sample format. The CSP may modify the format as necessary to comply with its internal policies and FedRAMP requirements.

ATTACHMENT 10 - FIPS 199

All Authorization Packages must include a Federal Information Processing Standard (FIPS) 199 Section, which will be reviewed for quality. This attachment has been provided separately to 3PAO.

The FIPS-199 Categorization report includes the determination of the security impact level for the cloud environment that may host any or all of the service models: IaaS, PaaS and SaaS. The ultimate goal of the security categorization is for the CSP to be able to select and implement the FedRAMP security controls applicable to its environment.

### Introduction and Purpose

This section is intended to be used by service providers who are applying for an Authorization through the U.S. federal government FedRAMP program.

The Federal Information Processing Standard 199 (FIPS 199) Categorization (Security Categorization) report is a key document in the security authorization package developed for submission to the Federal Risk and Authorization Management Program (FedRAMP) authorizing officials. The FIPS199 Categorization report includes the determination of the security impact level for the cloud environment that may host any or all of the service models (Information as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). The ultimate goal of the security categorization is for the cloud service provider (CSP) to be able to select and implement the FedRAMP security controls applicable to its environment.

The purpose of the FIPS199 Categorization report is for the CSP to assess and complete the categorization of their cloud environment, to provide the categorization to the System Owner/Certifier and the FedRAMP Joint Authorization Board (JAB) and in helping them to make a determination of the CSP’s ability to host systems at that level. The completed security categorization report will aid the CSP in selection and implementation of FedRAMP security controls at the determined categorization level.

### Scope

The scope of the FIPS199 Categorization report includes the assessment of the information type categories as defined in the NIST Special Publication 800-60 Volume II Revision 1 Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories.

### System Description

The Office 365 MultiTenant Cloud system has been determined to have a security categorization of Moderate.

Office 365 MT is a multi-tenant cloud computing-based subscription service offering from Microsoft. Cloud computing has been defined by NIST as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or cloud provider interaction. Further, as defined within NIST SP 800-145 (The NIST Definition of Cloud Computing), the service model for Office 365 MT is Software-as-a-Service (SaaS). SaaS is a model of software deployment whereby one or more applications and the computational resources to run them are provided for use on demand as a turnkey service. Its main purpose is to reduce the total cost of hardware and software development, maintenance, and operations. Security provisions are carried out mainly by the cloud provider. The cloud subscriber does not manage or control the underlying cloud infrastructure or individual applications, except for preference selections and limited administrative application settings.

Office 365 MT provides customers with cloud versions of Exchange Online (EXO), SharePoint Online (SPO) (including Project Online and OneDrive for Business), and Skype for Business (SFB). Exchange Online is an email service. SharePoint Online is a solution for creating sites to share documents and information. Skype for Business is a communication service that offers instant messaging, audio and video calling, online meetings, and web conferencing capabilities.

Office 365 MT has a number of supporting services in addition to these core, customer-facing services. Each core and supporting service is supported by a unique group of developers, testers, and administrators referred to throughout this document as a “service team”. Each service is deployed onto service-specific servers, whether physical or virtual.

### Methodology

Impact levels are determined for each information type based on the security objectives (confidentiality, integrity, availability). The confidentiality, integrity, and availability impact levels define the security sensitivity category of each information type. The FIPS PUB 199 is the high watermark for the impact level of all the applicable information types.

The FIPS PUB 199 analysis represents the information type and sensitivity levels of the CSP’s cloud service offering (and is not intended to include sensitivity levels of agency data). Customer agencies will be expected to perform a separate FIPS 199 Categorization report analysis for their own data hosted on the CSP’s cloud environment. The analysis must be added as an appendix to the SSP and drive the results for the Categorization section.

The Table 15‑8 CSP Applicable Information Types with Security Impact Levels Using NIST SP 800-60 V2 R1below uses the NIST SP 800-60 V2 R1 Volume II Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories to identify information types with the security impacts.

Table 15‑8 CSP Applicable Information Types with Security Impact Levels Using NIST SP 800-60 V2 R1

| Information Type | NIST SP 800-60 V2 R1  Recommended Confidentiality Impact Level | NIST SP 800-60 V2 R1  Recommended Integrity Impact Level | NIST SP 800-60 V2 R1  Recommended Availability Impact Level | CSP Selected Confidentiality Impact Level | CSP Selected Integrity Impact Level | CSP Selected Availability Impact Level | Statement  for Impact Adjustment Justification |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Lifecycle/Change Management | Low | Moderate | Low |  |  |  |  |
| System Maintenance | Low | Moderate | Low |  |  |  |  |
| IT Infrastructure Maintenance | Low | Low | Low |  |  |  |  |
| Information Security | Low | Moderate | Low |  |  |  |  |
| Record Retention | Low | Low | Low | Moderate | Low | Low | According to NIST 800-60: in cases where more sensitive information is involved, it will most commonly be personal information subject to the Privacy Act of 1974 or information that is proprietary to a corporation or other organization. Such information will often be assigned a moderate confidentiality impact level. |
| Information Management | Low | Moderate | Low | Moderate | Moderate | Low | According to NIST 800-60: information collection and storage involve the day-to-day processes of gathering and storing data from agency programs, partners, and stakeholders. More sensitive information being managed is usually personal information subject to the Privacy Act of 1974 or information that is proprietary to a corporation or other organization. Such information will often be assigned a moderate confidentiality impact level. |
| System and Network Monitoring | Moderate | Moderate | Low |  |  |  |  |
| Information Sharing | N/A | N/A | N/A |  |  |  |  |
| Lifecycle/Change Management | Low | Moderate | Low |  |  |  |  |
| System Maintenance | Low | Moderate | Low |  |  |  |  |
| IT Infrastructure Maintenance | Low | Low | Low |  |  |  |  |
| Information Security | Low | Moderate | Low |  |  |  |  |
| Record Retention | Low | Low | Low | Moderate | Low | Low | According to NIST 800-60: in cases where more sensitive information is involved, it will most commonly be personal information subject to the Privacy Act of 1974 or information that is proprietary to a corporation or other organization. Such information will often be assigned a moderate confidentiality impact level. |
| System and Network Monitoring | Moderate | Moderate | Low |  |  |  |  |
| Information Sharing | N/A | N/A | N/A |  |  |  |  |

ATTACHMENT 11 - Separation of Duties Matrix

All Authorization Packages have the option to provide a Separation of Duties Matrix attachment, which will be reviewed for quality.

**The 3PAO has been granted permission to view the Separation of Duties Matrix onsite.**

ATTACHMENT 12 – FedRAMP Laws and Regulations

The Table 15‑8 FedRAMP Templates that Reference FedRAMP Laws and Regulations Standards and Guidance lists all of the FedRAMP templates in which FedRAMP laws, regulations, standards and guidance are referenced. This attachment has been provided separately to 3PAO.

Table 15‑9 FedRAMP Templates that Reference FedRAMP Laws and Regulations Standards and Guidance

| Phase | | Document Title | |
| --- | --- | --- | --- |
| Document Phase | | SSP | System Security Plan |
|  | SSP Attachment 4 | PTA/PIA | Privacy Threshold Analysis and Privacy Impact Assessment |
|  | SSP Attachment 6 | ISCP | Information System Contingency Plan |
|  | SSP Attachment 10 | FIPS 199 | FIPS 199 Categorization |
| Assess Phase | | SAP | Security Assessment Plan |
| Authorize Phase | | SAR | Security Assessment Report |

The FedRAMP Laws and Regulations can be submitted as an appendix or an attachment. The attachment can be found on this page: Templates.

Note: All NIST Computer Security Publications can be found at the following  
URL: http://csrc.nist.gov/publications/PubsSPs.html

ATTACHMENT 13 – FedRAMP Inventory Workbook

All Authorization Packages must the Inventory attachment, which will be reviewed for quality. This attachment has been provided separately to 3PAO.

When completed, FedRAMP will accept this inventory workbook as the inventory information required by the following:

- System Security Plan

- Security Assessment Plan

- Security Assessment Report

- Information System Contingency Plan

- Initial POAM

- Monthly Continuous Monitoring (POAM or as a separate document)

The FedRAMP Inventory Workbook can be found on the following FedRAMP website page: Templates.

Note: A complete and detailed list of the system hardware and software inventory is required per NIST SP 800-53, Rev 4 CM-8.

ATTACHMENT 14 – Ports, Protocols and Services

The Ports, Protocols & Services in use in Office 365 MT will be provided as an attachment. This attachment has been provided separately to 3PAO.

ATTACHMENT 15 – Office 365 Internal Documents

This section is to list the Office 365 internal documents noted in this SSP that are onsite for auditor review. It is not a separate attachment.

Table ‑10 Office 365 Internal Documents

|  |
| --- |
| **Document Name** |
| Microsoft Documentation Retention Policy |
| Microsoft Enterprise Online Services Data Taxonomy (aka Asset Classification Standard) |
| Office 365 Data Handling Standard |
| Active Framework Controls |
| Office 365 Risk Management SOP |
| Office 365 MT Standard Operating Procedures (SOPs) |
| Office 365 Continuous Monitoring Strategy Guide |

1. FBI’s Criminal Justice Information Service (CJIS), United States Citizenship verification, FBI fingerprinting [↑](#footnote-ref-2)