Azure Blueprint FedRAMP System Security Plan (SSP) High Baseline Template

|  |
| --- |
|  |

CSP Name

Information System Name

Version #.#

Version Date

***Disclaimer:*** *The contents of this document are intended solely for the authorized user and contains confidential and/or privileged information - which is legally protected from disclosure. You are hereby notified that any use, dissemination, altering, copying, or storage of this document is strictly prohibited. This document is developed as a reference and should not be used to define all means by which a customer can meet specific compliance requirements and regulations. Customers should seek legal support from their organization on approved customer implementations.*

Controlled Unclassified Information

***Microsoft Guidance:***

*(Delete this section along with other instructions from your final version of this document.)*

*Azure’s Customer Responsibility Matrix (CRM) attachment denotes the list of controls alongside the control implementation narrative for Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) customers respectively. The CRM is divided into three total sheets, the readme section which includes summary information for use, the IaaS section for controls specific to IaaS customer responsibility, and the PaaS section for controls specific to PaaS customer responsibility. Furthermore, the CRM is a tool for IaaS and PaaS customers to quickly scan, filter and otherwise view the customer responsibility for FedRAMP Accreditation.*

*The customer responsibility column of the PaaS and IaaS sections in the CRM provide implementation requirements for Agencies and 3rd Party providers. In the event an Agency or 3rd Party provider has external customers, control implementation responsibility may be passed on to those customers, where feasible. For example, Multifactor Authentication Implementation may be a requirement where it is not feasible for an Agency or 3rd Party provider to transfer such responsibility onto an external customer.*

*Additionally, Microsoft Azure has populated this template with guidance for completing the control implementation descriptions. The fields within each description include:*

*Responsible Role: The job title or role of the individual(s) responsible for ensuring that a control is implemented and functioning as described within the text. Multiple roles may be responsible for a single control. Controls inherited wholly or in part from Microsoft Azure should include “Microsoft Azure” as a responsible role.*

*Parameter: When a control requirement includes organizationally-defined parameter values, those values should be specified here. In some cases, FedRAMP has provided minimum requirements for the parameter values.*

*Implementation Status: Choose one of the following options.*

* *Implemented: If the control is fully in place and meets all requirements.*
* *Partially Implemented: If the control is only partially in place or does not meet all requirements. A plan for achieving full implementation should be included in the Plan of Action & Milestone documentation.*
* *Planned: If the control is not in place. A plan for achieving full implementation should be included in the Plan of Action & Milestone documentation.*
* *Alternative Implementation: If the organization does not meet the control requirements as stated but has alternative or mitigating controls that achieve the goals of the control.*
* *Not Applicable: If the control is not applicable within the environment. A description of why the requirement does not apply should be included.*

*Control Origination: See the FedRAMP-provided table (Table 13-2 Control Origination and Definitions) in section 13 of the template below. In addition, note the following:*

* *The CSP in this context is Microsoft. Controls for which Microsoft is responsible are marked as “Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization”.*
* *The customer in this context is your agency.*
* *In some cases, Microsoft Azure provides tools or configuration options to assist you in implementing one or more security controls. These controls do not need to be marked as Inherited unless Microsoft Azure directly performs some action on your behalf. For example:*
  + *In AC-2, AC-3, etc., you may use Microsoft’s Azure Active Directory (AAD) service to create and manage accounts, grant access to systems, etc. Because defining roles, implementing procedures for granting account access, configuring accounts within the Azure portal, and integrating these activities into your application is your responsibility, these controls are not inherited.*
  + *In the MA family, Microsoft Azure performs all relevant hardware maintenance duties within Microsoft Azure datacenters, so nearly all of these controls are inherited. You will only be responsible for setting your own maintenance policies and procedures, and for performing any remote maintenance activities relevant to your application.*

*Control Implementation Details: This is the full description of how the organization meets the control. This template is prepopulated with customer responsibility sections for IaaS and PaaS customers, as well as a Microsoft Azure implementation section.*

*The IaaS and PaaS Customer Responsibility sections summarize the relevant control requirements that the customer is responsible for implementing and provide guidance on writing a successful control response. Based on the responsibility listed for the service model, you should detail the implementation statement for the control.*

*Some controls are implemented in whole or in part by Microsoft Azure on behalf of IaaS or PaaS customers. In this case, there is a summary of Microsoft’s implementation of the control in the Microsoft Azure sections for IaaS and PaaS. Where applicable, links or references to Azure documentation or other security-related documentation are included.*

*In this template, Microsoft has only pre-selected checkboxes for controls that are inherited from Microsoft Azure for IaaS and PaaS. You should review and update checkboxes for all other controls as applicable for your system.*

Instruction: This template contains a number of features to facilitate data entry. As you go through the template entering data, you will see prompts for you to enter different types of data.

Repeatable Field

Some multiple-occurring data fields have been linked together and you need only enter the data once. Enter the data once; then click outside the data entry field and all occurrences of that field will be populated. For example, when you see “Information System Abbreviation” and replace it with your system abbreviation, all instances of the abbreviation throughout the document will be replaced with the value you entered. This document contains the following repeatable fields:

CSP Name

Information System Name

Version Number

Version Date

Information System Abbreviation

If you find a data field from the above list that has not populated, then press the F9 key to refresh the data. If you make a change to one of the above data fields, you may also have to press the F9 key to refresh the data throughout the document. Remember to save the document after refreshes. The one exception to the repeatable fields is information system names for FedRAMP or leveraged authorizations that are identified as “Leveraged information system name:

Date Selection

Data fields that must contain a date will present a date selection menu.

Item Choice

Data fields that have a limited number of value choices will present a selection list.

Number Entry

Data fields that must have numeric values display “number.”

Text Entry

Many data fields, particularly in tables, that can contain any text display “Enter text” or “Click here to enter text.”

Delete this instruction from your final version of this document.

System Security Plan

Prepared by

| Identification of Organization that Prepared this Document | | |
| --- | --- | --- |
|  | Organization Name | <Enter Company/Organization>. |
| Street Address | <Enter Street Address> |
| Suite/Room/Building | <Enter Suite/Room/Building> |
| City, State Zip | <Enter Zip Code> |

Prepared for

| Identification of Cloud Service Provider | | |
| --- | --- | --- |
|  | Organization Name | <Enter Company/Organization>. |
| Street Address | <Enter Street Address> |
| Suite/Room/Building | <Enter Suite/Room/Building> |
| City, State Zip | <Enter Zip Code> |

Record of Changes

| Date | Description |
| --- | --- |
| 6/20/2016 | Original publication |
| 10/21/2016 | Removed tables in Sec 15.12 FedRAMP Laws and Regulations  Removed revision history tables in all of Sec 15  Removed Acronyms - see FedRAMP Master Acronyms and Glossary resource document  Added PTA to Sec 15.4 PTA and PIA  Added E-Authentication to Sec 15.3  Added FIPs to Sec 15.10 FIPS 199  Changed Inventory instruction and guidance Section 10 and Attachment 13  Removed chapter numbers from Attachments  Removed 3 questions from Sec 2.3 E-Authentication Determination |
| 6/6/2017 | Updated logo |
| 9/28/2017 | Updated IaaS, PaaS, and Microsoft responsibilities. |

Revision History

| Date | Description | Version of SSP | Author |
| --- | --- | --- | --- |
| <Date> | <Revision Description> | <Version> | <Author> |
| <Date> | <Revision Description> | <Version> | <Author> |

How to contact us

For questions about FedRAMP, or for technical questions about this document including how to use it, contact [*info@FedRAMP.gov*](mailto:info@fedramp.gov)

For more information about the FedRAMP project, see [www.FedRAMP.gov](http://www.fedramp.gov)

Instruction: The System Security Plan is the main document in which the Cloud Service Provider (CSP) describes all the security controls in use on the information system and their implementation.

This document is released in template format. Once populated with content, this document will include detailed information about service provider information security controls.

This document is intended to be used by service providers who are applying for a Joint Authorization Board (JAB) Provisional Authorization to Operate (P-ATO) through the Federal Risk and Authorization Management Program (FedRAMP) U.S. Federal agencies may want to use it to document information systems security plans that are not part of the FedRAMP program.

Delete this instruction from your final version of this document.

Table of Contents

[1 Information System Name/Title 1](#_Toc464802039)

[2 Information System Categorization 1](#_Toc464802040)

[2.1 Information Types 1](#_Toc464802041)

[2.2 Security Objectives Categorization (FIPS 199) 3](#_Toc464802042)

[2.3 E-Authentication Determination 3](#_Toc464802043)

[3 Information System Owner 4](#_Toc464802044)

[4 Authorizing Official 4](#_Toc464802045)

[5 Other Designated Contacts 4](#_Toc464802046)

[6 Assignment of Security Responsibility 5](#_Toc464802047)

[7 Information System Operational Status 6](#_Toc464802048)

[8 Information System Type 7](#_Toc464802049)

[8.1 Cloud Service Models 7](#_Toc464802050)

[8.2 Cloud Deployment Models 8](#_Toc464802051)

[8.3 Leveraged Authorizations 8](#_Toc464802052)

[9 General System Description 9](#_Toc464802053)

[9.1 System Function or Purpose 9](#_Toc464802054)

[9.2 Information System Components and Boundaries 9](#_Toc464802055)

[9.3 Types of Users 9](#_Toc464802056)

[9.4 Network Architecture 11](#_Toc464802057)

[10 System Environment And Inventory 11](#_Toc464802058)

[10.1 Data Flow 13](#_Toc464802059)

[10.2 Ports, Protocols and Services 13](#_Toc464802060)

[11 System Interconnections 15](#_Toc464802061)

[12 Laws, Regulations, Standards and Guidance 16](#_Toc464802062)

[12.1 Applicable Laws and Regulations 16](#_Toc464802063)

[12.2 Applicable Standards and Guidance 16](#_Toc464802064)

[13 Minimum Security Controls 17](#_Toc464802065)

[13.1 Access Control (AC) 25](#_Toc464802066)

[AC-1 Access Control Policy and Procedures Requirements (H) 25](#_Toc464802067)

[AC-2 Account Management (H) 26](#_Toc464802068)

[AC-2 (1) Control Enhancement (M) (H) 28](#_Toc464802069)

[AC-2 (2) Control Enhancement (H) 29](#_Toc464802070)

[AC-2 (3) Control Enhancement (H) 29](#_Toc464802071)

[AC-2 (4) Control Enhancement (H) 30](#_Toc464802072)

[AC-2 (5) Control Enhancement (H) 31](#_Toc464802073)

[AC-2 (7) Control Enhancement (H) 31](#_Toc464802074)

[AC-2 (9) Control Enhancement (H) 32](#_Toc464802075)

[AC-2 (10) Control Enhancement (M) (H) 33](#_Toc464802076)

[AC-2 (11) Control Enhancement (H) 33](#_Toc464802077)

[AC-2 (12) Control Enhancement (H) 34](#_Toc464802078)

[AC-2 (13) Control Enhancement (H) 35](#_Toc464802079)

[AC-3 Access Enforcement (L) (M) (H) 36](#_Toc464802080)

[AC-4 Information Flow Enforcement (M) (H) 36](#_Toc464802081)

[AC-4 (8) Control Enhancement (H) 37](#_Toc464802082)

[AC-4 (21) Control Enhancement (M) (H) 38](#_Toc464802083)

[AC-5 Separation of Duties (M) (H) 38](#_Toc464802084)

[AC-6 Least Privilege (M) (H) 39](#_Toc464802085)

[AC-6 (1) Control Enhancement (H) 40](#_Toc464802086)

[AC-6 (2) Control Enhancement (M) (H) 40](#_Toc464802087)

[AC-6 (3) Control Enhancement (H) 41](#_Toc464802088)

[AC 6 (5) Control Enhancement (M) (H) 42](#_Toc464802089)

[AC-6 (7) Control Enhancement (H) 43](#_Toc464802090)

[AC-6 (8) Control Enhancement (H) 43](#_Toc464802091)

[AC-6 (9) Control Enhancement (M) (H) 44](#_Toc464802092)

[AC-6 (10) Control Enhancement (M) (H) 45](#_Toc464802093)

[AC-7 Unsuccessful Login Attempts (H) 45](#_Toc464802094)

[AC-7 (2) Control Enhancement (H) 46](#_Toc464802095)

[AC-8 System Use Notification (L) (M) (H) 47](#_Toc464802096)

[AC-10 Concurrent Session Control (M) (H) 49](#_Toc464802097)

[AC-11 Session Lock (M) (H) 50](#_Toc464802098)

[AC-11 (1) Control Enhancement (M) (H) 51](#_Toc464802099)

[AC-12 Session Termination (M) (H) 51](#_Toc464802100)

[AC-12 (1) Control Enhancement (H) 52](#_Toc464802101)

[AC-14 Permitted Actions without Identification or Authentication (L) (M) (H) 53](#_Toc464802102)

[AC-17 Remote Access (L) (M) (H) 54](#_Toc464802103)

[AC-17 (1) Control Enhancement (M) (H) 54](#_Toc464802104)

[AC-17 (2) Control Enhancement (M) (H) 55](#_Toc464802105)

[AC-17 (3) Control Enhancement (M) (H) 56](#_Toc464802106)

[AC-17 (4) Control Enhancement (M) (H) 56](#_Toc464802107)

[AC-17 (9) Control Enhancement (M) (H) 57](#_Toc464802108)

[AC-18 Wireless Access Restrictions (L) (M) (H) 58](#_Toc464802109)

[AC-18 (1) Control Enhancement (M) (H) 58](#_Toc464802110)

[AC-18 (3) Control Enhancement (H) 59](#_Toc464802111)

[AC-18 (4) Control Enhancement (H) 60](#_Toc464802112)

[AC-18 (5) Control Enhancement (H) 60](#_Toc464802113)

[AC-19 Access Control for Portable and Mobile Systems (L) (M) (H) 61](#_Toc464802114)

[AC-19 (5) Control Enhancement (M) (H) 61](#_Toc464802115)

[AC-20 Use of External Information Systems (L) (M) (H) 62](#_Toc464802116)

[AC-20 (1) Control Enhancement (M) (H) 63](#_Toc464802117)

[AC-20 (2) Control Enhancement (M) (H) 64](#_Toc464802118)

[AC-21 Information Sharing (M) (H) 64](#_Toc464802119)

[AC-22 Publicly Accessible Content (L) (M) (H) 65](#_Toc464802120)

[13.2 Awareness and Training (AT) 66](#_Toc464802121)

[AT-1 Security Awareness and Training Policy and Procedures (H) 66](#_Toc464802122)

[AT-2 Security Awareness (L) (M) (H) 67](#_Toc464802123)

[AT-2 (2) Control Enhancement (M) (H) 68](#_Toc464802124)

[AT-3 Role-Based Security Training (L) (M) (H) 68](#_Toc464802125)

[AT-3 (3) Control Enhancement (H) 69](#_Toc464802126)

[AT-3 (4) Control Enhancement (H) 70](#_Toc464802127)

[AT-4 Security Training Records (H) 70](#_Toc464802128)

[13.3 Audit and Accountability (AU) 71](#_Toc464802129)

[AU-1 Audit and Accountability Policy and Procedures (H) 71](#_Toc464802130)

[AU-2 Audit Events (L) (M) (H) 72](#_Toc464802131)

[AU-2 (3) Control Enhancement (M) (H) 73](#_Toc464802132)

[AU-3 Content of Audit Records (L) (M) (H) 74](#_Toc464802133)

[AU-3 (1) Control Enhancement (H) 75](#_Toc464802134)

[AU-3 (2) Control Enhancement (H) 76](#_Toc464802135)

[AU-4 Audit Storage Capacity (L) (M) (H) 76](#_Toc464802136)

[AU-5 Response to Audit Processing Failures (L) (M) (H) 77](#_Toc464802137)

[AU-5 (1) Control Enhancement (H) 78](#_Toc464802138)

[AU-5 (2) Control Enhancement (H) 78](#_Toc464802139)

[AU-6 Audit Review, Analysis, and Reporting (L) (M) (H) 79](#_Toc464802140)

[AU-6 (1) Control Enhancement (M) (H) 80](#_Toc464802141)

[AU-6 (3) Control Enhancement (M) (H) 81](#_Toc464802142)

[AU-6 (4) Control Enhancement (H) 81](#_Toc464802143)

[AU-6 (5) Control Enhancement (H) 82](#_Toc464802144)

[AU-6 (6) Control Enhancement (H) 83](#_Toc464802145)

[AU-6 (7) Control Enhancement (H) 83](#_Toc464802146)

[AU-6 (10) Control Enhancement (H) 84](#_Toc464802147)

[AU-7 Audit Reduction and Report Generation (M) (H) 85](#_Toc464802148)

[AU-7 (1) Control Enhancement (M) (H) 85](#_Toc464802149)

[AU-8 Time Stamps (L) (M) (H) 86](#_Toc464802150)

[AU-8 (1) Control Enhancement (M) (H) 87](#_Toc464802151)

[AU-9 Protection of Audit Information (L) (M) (H) 89](#_Toc464802152)

[AU-9 (2) Control Enhancement (M) (H) 89](#_Toc464802153)

[AU-9 (3) Control Enhancement (H) 90](#_Toc464802154)

[AU-9 (4) Control Enhancement (M) (H) 91](#_Toc464802155)

[AU-10 Non-repudiation (H) 91](#_Toc464802156)

[AU-11 Audit Record Retention (H) 92](#_Toc464802157)

[AU-12 Audit Generation (L) (M) (H) 93](#_Toc464802158)

[AU-12 (1) Control Enhancement (H) 94](#_Toc464802159)

[AU-12 (3) Control Enhancement (H) 94](#_Toc464802160)

[13.4 Security Assessment and Authorization (CA) 95](#_Toc464802161)

[CA-1 Certification, Authorization, Security Assessment Policy and Procedures (H) 95](#_Toc464802162)

[CA-2 Security Assessments (L) (M) (H) 96](#_Toc464802163)

[CA-2 (1) Control Enhancement (L) (M) (H) 97](#_Toc464802164)

[CA-2 (2) Control Enhancement (M) (H) 98](#_Toc464802165)

[CA-2 (3) Control Enhancement (M) (H) 99](#_Toc464802166)

[CA-3 System Interconnections (L) (M) (H) 100](#_Toc464802167)

[CA-3 (3) Control Enhancement (M) (H) 101](#_Toc464802168)

[CA-3 (5) Control Enhancement (H) 102](#_Toc464802169)

[CA-5 Plan of Action and Milestones (L) (M) (H) 102](#_Toc464802170)

[CA-6 Security Authorization (L) (M) (H) 103](#_Toc464802171)

[CA-7 Continuous Monitoring (L) (M) (H) 104](#_Toc464802172)

[CA-7 (1) Control Enhancement (M) (H) 106](#_Toc464802173)

[CA-7 (3) Control Enhancement (H) 107](#_Toc464802174)

[CA-8 Penetration Testing (M) (H) 108](#_Toc464802175)

[CA-8 (1) Control Enhancement (M) (H) 108](#_Toc464802176)

[CA-9 Internal System Connections (L) (M) (H) 109](#_Toc464802177)

[13.5 Configuration Management (CM) 110](#_Toc464802178)

[CM-1 Configuration Management Policies and Procedures (H) 110](#_Toc464802179)

[CM-2 Baseline Configuration (L) (M) (H) 111](#_Toc464802180)

[CM-2 (1) Control Enhancement (H) 111](#_Toc464802181)

[CM-2 (2) Control Enhancement (M) (H) 112](#_Toc464802182)

[CM-2 (3) Control Enhancement (H) 113](#_Toc464802183)

[CM-2 (7) Control Enhancement (M) (H) 114](#_Toc464802184)

[CM-3 Configuration Change Control (M) (H) 114](#_Toc464802185)

[CM-3 (1) Control Enhancement (H) 116](#_Toc464802186)

[CM-3 (2) Control Enhancement (M)(H) 117](#_Toc464802187)

[CM-3 (4) Enhancement (H) 118](#_Toc464802188)

[CM-3 (6) Enhancement (H) 118](#_Toc464802189)

[CM-4 Security Impact Analysis (L) (M) (H) 119](#_Toc464802190)

[CM-4 (1) Control Enhancement (H) 120](#_Toc464802191)

[CM-5 Access Restrictions for Change (M) (H) 120](#_Toc464802192)

[CM-5 (1) Control Enhancement (M) (H) 121](#_Toc464802193)

[CM-5 (2) Control Enhancement (H) 121](#_Toc464802194)

[CM-5 (3) Control Enhancement (M) (H) 122](#_Toc464802195)

[CM-5 (5) Control Enhancement (M) (H) 123](#_Toc464802196)

[CM-6 Configuration Settings (L) (M) (H) 124](#_Toc464802197)

[CM-6 (1) Control Enhancement (M) (H) 125](#_Toc464802198)

[CM-6 (2) Control Enhancement (H) 126](#_Toc464802199)

[CM-7 Least Functionality (L) (M) (H) 126](#_Toc464802200)

[CM-7 (1) Control Enhancement (M) (H) 127](#_Toc464802201)

[CM-7 (2) Control Enhancement (M) (H) 128](#_Toc464802202)

[CM-7 (5) Control Enhancement (H) 129](#_Toc464802203)

[CM-8 Information System Component Inventory (L) (M) (H) 130](#_Toc464802204)

[CM-8 (1) Control Enhancement (M) (H) 131](#_Toc464802205)

[CM-8 (2) Control Enhancement (H) 131](#_Toc464802206)

[CM-8 (3) Control Enhancement (M) (H) 132](#_Toc464802207)

[CM-8 (4) Control Enhancement (H) 133](#_Toc464802208)

[CM-8 (5) Control Enhancement (M) (H) 133](#_Toc464802209)

[CM-9 Configuration Management Plan (M) (H) 134](#_Toc464802210)

[CM-10 Software Usage Restrictions (L) (M) (H) 135](#_Toc464802211)

[CM-10 (1) Control Enhancement (M) (H) 136](#_Toc464802212)

[CM-11 User-Installed Software (M) (H) 136](#_Toc464802213)

[CM-11 (1) Control Enhancement (H) 137](#_Toc464802214)

[13.6 Contingency Planning (CP) 138](#_Toc464802215)

[CP-1 Contingency Planning Policy and Procedures (H) 138](#_Toc464802216)

[CP-2 Contingency Plan (L) (M) (H) 139](#_Toc464802217)

[CP-2 (1) Control Enhancement (M) (H) 140](#_Toc464802218)

[CP-2 (2) Control Enhancement (M) (H) 141](#_Toc464802219)

[CP-2 (3) Control Enhancement (M) (H) 142](#_Toc464802220)

[CP-2 (4) Control Enhancement (H) 142](#_Toc464802221)

[CP-2 (5) Control Enhancement (H) 143](#_Toc464802222)

[CP-2 (8) Control Enhancement (M) (H) 144](#_Toc464802223)

[CP-3 Contingency Training (L) (M) (H) 144](#_Toc464802224)

[CP-3 (1) Control Enhancement (H) 145](#_Toc464802225)

[CP-4 Contingency Plan Testing (H) 146](#_Toc464802226)

[CP-4 (1) Control Enhancement (M) (H) 146](#_Toc464802227)

[CP-4 (2) Control Enhancement (H) 147](#_Toc464802228)

[CP-6 Alternate Storage Site (M) (H) 148](#_Toc464802229)

[CP-6 (1) Control Enhancement (M) (H) 148](#_Toc464802230)

[CP-6 (2) Control Enhancement (H) 149](#_Toc464802231)

[CP-6 (3) Control Enhancement (M) (H) 150](#_Toc464802232)

[CP-7 Alternate Processing Site (M) (H) 150](#_Toc464802233)

[CP-7 (1) Control Enhancement (M) (H) 151](#_Toc464802234)

[CP-7 (2) Control Enhancement (M) (H) 152](#_Toc464802235)

[CP-7 (3) Control Enhancement (M) (H) 153](#_Toc464802236)

[CP-7 (4) Control Enhancement (H) 153](#_Toc464802237)

[CP-8 Telecommunications Services (M) (H) 154](#_Toc464802238)

[CP-8 (1) Control Enhancement (M) (H) 155](#_Toc464802239)

[CP-8 (2) Control Enhancement (M) (H) 155](#_Toc464802240)

[CP-8 (3) Control Enhancement (H) 156](#_Toc464802241)

[CP-8 (4) Control Enhancement (H) 157](#_Toc464802242)

[CP-9 Information System Backup (L) (M) (H) 157](#_Toc464802243)

[CP-9 (1) Control Enhancement (H) 159](#_Toc464802244)

[CP-9 (2) Control Enhancement (H) 159](#_Toc464802245)

[CP-9 (3) Control Enhancement (M) (H) 160](#_Toc464802246)

[CP-9 (5) Control Enhancement (H) 161](#_Toc464802247)

[CP-10 Information System Recovery and Reconstitution (L) (M) (H) 161](#_Toc464802248)

[CP-10 (2) Control Enhancement (M) (H) 162](#_Toc464802249)

[CP-10 (4) Control Enhancement (H) 163](#_Toc464802250)

[13.7 Identification and Authentication (IA) 163](#_Toc464802251)

[IA-1 Identification and Authentication Policy and Procedures (H) 163](#_Toc464802252)

[IA-2 User Identification and Authentication (L) (M) (H) 164](#_Toc464802253)

[IA-2 (1) Control Enhancement (L) (M) (H) 165](#_Toc464802254)

[IA-2 (2) Control Enhancement (M) (H) 165](#_Toc464802255)

[IA-2 (3) Control Enhancement (M) (H) 166](#_Toc464802256)

[IA-2 (4) Control Enhancement (H) 167](#_Toc464802257)

[IA-2 (5) Control Enhancement (M) (H) 167](#_Toc464802258)

[IA-2 (8) Control Enhancement (M) (H) 168](#_Toc464802259)

[IA-2 (9) Control Enhancement (H) 168](#_Toc464802260)

[IA-2 (11) Control Enhancement (M) (H) 169](#_Toc464802261)

[IA-2 (12) Control Enhancement (L) (M) (H) 170](#_Toc464802262)

[IA-3 Device Identification and Authentication (M) (H) 171](#_Toc464802263)

[IA-4 Identifier Management (H) 171](#_Toc464802264)

[IA-4 (4) Control Enhancement (M) (H) 172](#_Toc464802265)

[IA-5 Authenticator Management (H) 173](#_Toc464802266)

[IA-5 (1) Control Enhancement (H) 175](#_Toc464802267)

[IA-5 (2) Control Enhancement (M) (H) 176](#_Toc464802268)

[IA-5 (3) Control Enhancement (M) (H) 177](#_Toc464802269)

[IA-5 (4) Control Enhancement (H) 177](#_Toc464802270)

[IA-5 (6) Control Enhancement (M) (H) 178](#_Toc464802271)

[IA-5 (7) Control Enhancement (M) (H) 179](#_Toc464802272)

[IA-5 (8) Control Enhancement (H) 179](#_Toc464802273)

[IA-5 (11) Control Enhancement (L) (M) (H) 180](#_Toc464802274)

[IA-5 (13) Control Enhancement (H) 181](#_Toc464802275)

[IA-6 Authenticator Feedback (L) (M) (H) 181](#_Toc464802276)

[IA-7 Cryptographic Module Authentication (L) (M) (H) 182](#_Toc464802277)

[IA-8 Identification and Authentication (Non-Organizational Users) (L) (M) (H) 183](#_Toc464802278)

[IA-8 (1) Control Enhancement (L) (M) (H) 183](#_Toc464802279)

[IA-8 (2) Control Enhancement (L) (M) (H) 184](#_Toc464802280)

[IA-8 (3) Control Enhancement (L) (M) (H) 184](#_Toc464802281)

[IA-8 (4) Control Enhancement (L) (M) (H) 185](#_Toc464802282)

[13.8 Incident Response (IR) 186](#_Toc464802283)

[IR-1 Incident Response Policy and Procedures (H) 186](#_Toc464802284)

[IR-2 Incident Response Training (H) 186](#_Toc464802285)

[IR-2 (1) Control Enhancement (H) 187](#_Toc464802286)

[IR-2 (2) Control Enhancement (H) 188](#_Toc464802287)

[IR-3 Incident Response Testing (H) 188](#_Toc464802288)

[IR-3 (2) Control Enhancement (M) (H) 189](#_Toc464802289)

[IR-4 Incident Handling (L) (M) (H) 190](#_Toc464802290)

[IR-4 (1) Control Enhancement (M) (H) 191](#_Toc464802291)

[IR-4 (2) Control Enhancement (H) 191](#_Toc464802292)

[IR-4 (3) Control Enhancement (H) 192](#_Toc464802293)

[IR-4 (4) Control Enhancement (H) 193](#_Toc464802294)

[IR-4 (6) Control Enhancement (H) 193](#_Toc464802295)

[IR-4 (8) Control Enhancement (H) 194](#_Toc464802296)

[IR-5 Incident Monitoring (L) (M) (H) 195](#_Toc464802297)

[IR-5 (1) Control Enhancement (H) 195](#_Toc464802298)

[IR-6 Incident Reporting (L) (M) (H) 196](#_Toc464802299)

[IR-6 (1) Control Enhancement (M) (H) 197](#_Toc464802300)

[IR-7 Incident Response Assistance (L) (M) (H) 197](#_Toc464802301)

[IR-7 (1) Control Enhancement (M) (H) 198](#_Toc464802302)

[IR-7 (2) Control Enhancement (M) (H) 199](#_Toc464802303)

[IR-8 Incident Response Plan (L) (M) (H) 199](#_Toc464802304)

[IR-9 Information Spillage Response (M) (H) 201](#_Toc464802305)

[IR-9 (1) Control Enhancement (M) (H) 202](#_Toc464802306)

[IR-9 (2) Control Enhancement (H) 203](#_Toc464802307)

[IR-9 (3) Control Enhancement (M) (H) 203](#_Toc464802308)

[IR-9 (4) Control Enhancement (M) (H) 204](#_Toc464802309)

[13.9 Maintenance (MA) 205](#_Toc464802310)

[MA-1 System Maintenance Policy and Procedures (H) 205](#_Toc464802311)

[MA-2 Controlled Maintenance (L) (M) (H) 205](#_Toc464802312)

[MA-2 (2) Control Enhancement (H) 207](#_Toc464802313)

[MA-3 Maintenance Tools (M) (H) 207](#_Toc464802314)

[MA-3 (1) Control Enhancement (M) (H) 208](#_Toc464802315)

[MA-3 (2) Control Enhancement (M) (H) 209](#_Toc464802316)

[MA-3 (3) Control Enhancement (M) (H) 209](#_Toc464802317)

[MA-4 Remote Maintenance (L) (M) (H) 210](#_Toc464802318)

[MA-4 (2) Control Enhancement (M) (H) 211](#_Toc464802319)

[MA-4 (3) Control Enhancement (H) 212](#_Toc464802320)

[MA-4 (6) Enhancement (H) 213](#_Toc464802321)

[MA-5 Maintenance Personnel (L) (M) (H) 213](#_Toc464802322)

[MA-5 (1) Control Enhancement (H) 214](#_Toc464802323)

[MA-6 Timely Maintenance (M) (H) 215](#_Toc464802324)

[13.10 Media Protection (MP) 216](#_Toc464802325)

[MP-1 Media Protection Policy and Procedures (H) 216](#_Toc464802326)

[MP-2 Media Access (H) 217](#_Toc464802327)

[MP-3 Media Labeling (M) (H) 217](#_Toc464802328)

[MP-4 Media Storage (M) (H) 218](#_Toc464802329)

[MP-5 Media Transport (M) (H) 219](#_Toc464802330)

[MP-5 (4) Control Enhancement (M) (H) 220](#_Toc464802331)

[MP-6 Media Sanitization and Disposal (H) 221](#_Toc464802332)

[MP-6 (1) Control Enhancement (H) 221](#_Toc464802333)

[MP-6 (2) Control Enhancement (H) 222](#_Toc464802334)

[MP-6 (3) Control Enhancement (H) 223](#_Toc464802335)

[MP-7 Media Use (L) (M) (H) 223](#_Toc464802336)

[MP-7 (1) Control Enhancement (M) (H) 224](#_Toc464802337)

[13.11 Physical and Environmental Protection (PE) 225](#_Toc464802338)

[PE-1 Physical and Environmental Protection Policy and Procedures (H) 225](#_Toc464802339)

[PE-2 Physical Access Authorizations (H) 226](#_Toc464802340)

[PE-3 Physical Access Control (L) (M) (H) 227](#_Toc464802341)

[PE-3 (1) Control Enhancement (H) 228](#_Toc464802342)

[PE-4 Access Control for Transmission Medium (M) (H) 229](#_Toc464802343)

[PE-5 Access Control for Output Devices (M) (H) 230](#_Toc464802344)

[PE-6 Monitoring Physical Access (L) (M) (H) 230](#_Toc464802345)

[PE-6 (1) Control Enhancement (M) (H) 231](#_Toc464802346)

[PE-6 (4) Control Enhancement (H) 232](#_Toc464802347)

[PE-8 Visitor Access Records (L) (M) (H) 232](#_Toc464802348)

[PE-8 (1) Control Enhancement (H) 233](#_Toc464802349)

[PE-9 Power Equipment and Cabling (M) (H) 234](#_Toc464802350)

[PE-10 Emergency Shutoff (M) (H) 234](#_Toc464802351)

[PE-11 Emergency Power (M) (H) 235](#_Toc464802352)

[PE-11 (1) Control Enhancement (H) 236](#_Toc464802353)

[PE-12 Emergency Lighting (L) (M) (H) 236](#_Toc464802354)

[PE-13 Fire Protection (L) (M) (H) 237](#_Toc464802355)

[PE-13 (1) Control Enhancement (H) 238](#_Toc464802356)

[PE-13 (2) Control Enhancement (M) (H) 238](#_Toc464802357)

[PE-13 (3) Control Enhancement (M) (H) 239](#_Toc464802358)

[PE-14 Temperature and Humidity Controls (L) (M) (H) 240](#_Toc464802359)

[PE-14 (2) Control Enhancement (M) (H) 240](#_Toc464802360)

[PE-15 Water Damage Protection (L) (M) (H) 241](#_Toc464802361)

[PE-15 (1) Control Enhancement (H) 242](#_Toc464802362)

[PE-16 Delivery and Removal (L) (M) (H) 242](#_Toc464802363)

[PE-17 Alternate Work Site (M) (H) 243](#_Toc464802364)

[PE-18 Location of Information System Components (H) 244](#_Toc464802365)

[13.12 Planning (PL) 244](#_Toc464802366)

[PL-1 Security Planning Policy and Procedures (H) 244](#_Toc464802367)

[PL-2 System Security Plan (L) (M) (H) 245](#_Toc464802368)

[PL-2 (3) Control Enhancement (M) (H) 247](#_Toc464802369)

[PL-4 Rules of Behavior (H) 247](#_Toc464802370)

[PL-4 (1) Control Enhancement (M) (H) 248](#_Toc464802371)

[PL-8 Information Security Architecture (M) (H) 249](#_Toc464802372)

[13.13 Personnel Security (PS) 250](#_Toc464802373)

[PS-1 Personnel Security Policy and Procedures (H) 250](#_Toc464802374)

[PS-2 Position Categorization (H) 251](#_Toc464802375)

[PS-3 Personnel Screening (L) (M) (H) 252](#_Toc464802376)

[PS-3 (3) Control Enhancement (M) (H) 253](#_Toc464802377)

[PS-4 Personnel Termination (H) 253](#_Toc464802378)

[PS-4 (2) Control Enhancement (H) 254](#_Toc464802379)

[PS-5 Personnel Transfer (H) 255](#_Toc464802380)

[PS-6 Access Agreements (H) 256](#_Toc464802381)

[PS-7 Third-Party Personnel Security (H) 257](#_Toc464802382)

[PS-8 Personnel Sanctions (H) 258](#_Toc464802383)

[13.14 Risk Assessment (RA) 259](#_Toc464802384)

[RA-1 Risk Assessment Policy and Procedures (H) 259](#_Toc464802385)

[RA-2 Security Categorization (L) (M) (H) 260](#_Toc464802386)

[RA-3 Risk Assessment (H) 261](#_Toc464802387)

[RA-5 Vulnerability Scanning (L) (M) (H) 262](#_Toc464802388)

[RA-5 (1) Control Enhancement (M) (H) 263](#_Toc464802389)

[RA-5 (2) Control Enhancement (M) (H) 264](#_Toc464802390)

[RA-5 (3) Control Enhancement (M) (H) 265](#_Toc464802391)

[RA-5 (4) Control Enhancement (H) 265](#_Toc464802392)

[RA-5 (5) Control Enhancement (M) (H) 266](#_Toc464802393)

[RA-5 (6) Control Enhancement (M) (H) 267](#_Toc464802394)

[RA-5 (8) Control Enhancement (L) (M) (H) 267](#_Toc464802395)

[RA-5 (10) Control Enhancement (H) 268](#_Toc464802396)

[13.15 System and Services Acquisition (SA) 269](#_Toc464802397)

[SA-1 System and Services Acquisition Policy and Procedures (H) 269](#_Toc464802398)

[SA-2 Allocation of Resources (L) (M) (H) 270](#_Toc464802399)

[SA-3 System Development Life Cycle (L) (M) (H) 270](#_Toc464802400)

[SA-4 Acquisitions Process (L) (M) (H) 271](#_Toc464802401)

[SA-4 (1) Control Enhancement (M) (H) 273](#_Toc464802402)

[SA-4 (2) Control Enhancement (H) 273](#_Toc464802403)

[SA-4 (8) Control Enhancement (M) (H) 274](#_Toc464802404)

[SA-4 (9) Control Enhancement (M) (H) 275](#_Toc464802405)

[SA-4 (10) Control Enhancement (M) (H) 275](#_Toc464802406)

[SA-5 Information System Documentation (H) 276](#_Toc464802407)

[SA-8 Security Engineering Principles (M) (H) 277](#_Toc464802408)

[SA-9 External Information System Services (L) (M) (H) 278](#_Toc464802409)

[SA-9 (1) Control Enhancement (M) (H) 279](#_Toc464802410)

[SA-9 (2) Control Enhancement (M) (H) 280](#_Toc464802411)

[SA-9 (4) Control Enhancement (M) (H) 280](#_Toc464802412)

[SA-9 (5) Control Enhancement (M) (H) 281](#_Toc464802413)

[SA-10 Developer Configuration Management (M) (H) 282](#_Toc464802414)

[SA-10 (1) Control Enhancement (M) (H) 283](#_Toc464802415)

[SA-11 Developer Security Testing and Evaluation (M) (H) 284](#_Toc464802416)

[SA-11 (1) Control Enhancement (M) (H) 285](#_Toc464802417)

[SA-11 (2) Control Enhancement (M) (H) 285](#_Toc464802418)

[SA-11 (8) Control Enhancement (M) (H) 286](#_Toc464802419)

[SA-12 Supply Chain Protection (H) 287](#_Toc464802420)

[SA-15 Development Process, Standards, and Tools (H) 287](#_Toc464802421)

[SA-16 Developer-Provided Training (H) 288](#_Toc464802422)

[SA-17 Developer Security Architecture and Design (H) 289](#_Toc464802423)

[13.16 System and Communications Protection (SC) 290](#_Toc464802424)

[SC-1 System and Communications Protection Policy and Procedures (H) 290](#_Toc464802425)

[SC-2 Application Partitioning (M) (H) 291](#_Toc464802426)

[SC-3 Security Function Isolation (H) 291](#_Toc464802427)

[SC-4 Information in Shared Resources (M) (H) 292](#_Toc464802428)

[SC-5 Denial of Service Protection (L) (M) (H) 293](#_Toc464802429)

[SC-6 Resource Availability (M) (H) 293](#_Toc464802430)

[SC-7 Boundary Protection (L) (M) (H) 294](#_Toc464802431)

[SC-7 (3) Control Enhancement (M) (H) 295](#_Toc464802432)

[SC-7 (4) Control Enhancement (H) 296](#_Toc464802433)

[SC-7 (5) Control Enhancement (M) (H) 297](#_Toc464802434)

[SC-7 (7) Control Enhancement (M) (H) 297](#_Toc464802435)

[SC-7 (8) Control Enhancement (M) (H) 298](#_Toc464802436)

[SC-7 (10) Control Enhancement (H) 298](#_Toc464802437)

[SC-7 (12) Control Enhancement (H) 299](#_Toc464802438)

[SC-7 (13) Control Enhancement (H) 300](#_Toc464802439)

[SC-7 (18) Control Enhancement (M) (H) 301](#_Toc464802440)

[SC-7 (20) Control Enhancement (H) 301](#_Toc464802441)

[SC-7 (21) Control Enhancement (H) 302](#_Toc464802442)

[SC-8 Transmission confidentiality and Integrity (M) (H) 303](#_Toc464802443)

[SC-8 (1) Control Enhancement (M) (H) 303](#_Toc464802444)

[SC-10 Network Disconnect (H) 304](#_Toc464802445)

[SC-12 Cryptographic Key Establishment & Management (L) (M) (H) 305](#_Toc464802446)

[SC-12 (1) Control Enhancement (H) 305](#_Toc464802447)

[SC-12 (2) Control Enhancement (M) (H) 306](#_Toc464802448)

[SC-12 (3) Control Enhancement (M) (H) 306](#_Toc464802449)

[SC-13 Use of Cryptography (L) (M) (H) 307](#_Toc464802450)

[SC-15 Collaborative Computing Devices (M) (H) 308](#_Toc464802451)

[SC-17 Public Key Infrastructure Certificates (M) (H) 309](#_Toc464802452)

[SC-18 Mobile Code (M) (H) 310](#_Toc464802453)

[SC-19 Voice Over Internet Protocol (M) (H) 311](#_Toc464802454)

[SC-20 Secure Name / Address Resolution Service (Authoritative Source) (L) (M) (H) 311](#_Toc464802455)

[SC-21 Secure Name / Address Resolution Service (Recursive or Caching Resolver) (L) (M) (H) 312](#_Toc464802456)

[SC-22 Architecture and Provisioning for Name / Address Resolution Service (L) (M) (H) 313](#_Toc464802457)

[SC-23 Session Authenticity (M) (H) 313](#_Toc464802458)

[SC-23 (1) Enhancement (H) 314](#_Toc464802459)

[SC-24 Fail in Known State (H) 315](#_Toc464802460)

[SC-28 Protection of Information at Rest (M) (H) 315](#_Toc464802461)

[SC-28 (1) Control Enhancement (H) 316](#_Toc464802462)

[SC-39 Process Isolation (L) (M) (H) 317](#_Toc464802463)

[13.17 System and Information Integrity (SI) 317](#_Toc464802464)

[SI-1 System and Information Integrity Policy and Procedures (H) 317](#_Toc464802465)

[SI-2 Flaw Remediation (L) (M) (H) 318](#_Toc464802466)

[SI-2 (1) Control Enhancement (H) 319](#_Toc464802467)

[SI-2 (2) Control Enhancement (M) (H) 320](#_Toc464802468)

[SI-2 (3) Control Enhancement (M) (H) 320](#_Toc464802469)

[SI-3 Malicious Code Protection (H) 321](#_Toc464802470)

[SI-3 (1) Control Enhancement (M) (H) 322](#_Toc464802471)

[SI-3 (2) Control Enhancement (M) (H) 323](#_Toc464802472)

[SI-3 (7) Control Enhancement (M) (H) 323](#_Toc464802473)

[SI-4 Information System Monitoring (L) (M) (H) 324](#_Toc464802474)

[SI-4 (1) Control Enhancement (M) (H) 325](#_Toc464802475)

[SI-4 (2) Control Enhancement (M) (H) 326](#_Toc464802476)

[SI-4 (4) Control Enhancement (M) (H) 327](#_Toc464802477)

[SI-4 (5) Control Enhancement (M) (H) 327](#_Toc464802478)

[SI-4 (11) Control Enhancement (H) 328](#_Toc464802479)

[SI-4 (14) Control Enhancement (M) (H) 329](#_Toc464802480)

[SI-4 (16) Control Enhancement (M) (H) 329](#_Toc464802481)

[SI-4 (18) Control Enhancement (H) 330](#_Toc464802482)

[SI-4 (19) Control Enhancement (H) 331](#_Toc464802483)

[SI-4 (20) Control Enhancement (H) 331](#_Toc464802484)

[SI-4 (22) Control Enhancement (H) 332](#_Toc464802485)

[SI-4 (23) Control Enhancement (M) (H) 333](#_Toc464802486)

[SI-4 (24) Control Enhancement (H) 333](#_Toc464802487)

[SI-5 Security Alerts & Advisories (L) (M) (H) 334](#_Toc464802488)

[SI-5 (1) Control Enhancement (H) 335](#_Toc464802489)

[SI-6 Security Functionality Verification (M) (H) 335](#_Toc464802490)

[SI-7 Software & Information Integrity (M) (H) 336](#_Toc464802491)

[SI-7 (1) Control Enhancement (M) (H) 337](#_Toc464802492)

[SI-7 (2) Control Enhancement (H) 338](#_Toc464802493)

[SI-7 (5) Control Enhancement (H) 338](#_Toc464802494)

[SI-7 (7) Control Enhancement (M) (H) 339](#_Toc464802495)

[SI-7 (14) Control Enhancement (H) 340](#_Toc464802496)

[SI-8 Spam Protection (M) (H) 340](#_Toc464802497)

[SI-8 (1) Control Enhancement (M) (H) 341](#_Toc464802498)

[SI-8 (2) Control Enhancement (M) (H) 342](#_Toc464802499)

[SI-10 Information Input Validation (M) (H) 342](#_Toc464802500)

[SI-11 Error Handling (M) (H) 343](#_Toc464802501)

[SI-12 Information Output Handling and Retention (L) (M) (H) 344](#_Toc464802502)

[SI-16 Memory Protection (M) (H) 344](#_Toc464802503)

[14 Acronyms 346](#_Toc464802504)

[15 Attachments 347](#_Toc464802505)

[ATTACHMENT 1 - Information Security Policies and Procedures 349](#_Toc464802506)

[ATTACHMENT 2 - User Guide 350](#_Toc464802507)

[ATTACHMENT 3 – e-Authentication Worksheet 351](#_Toc464802508)

[Introduction and Purpose 351](#_Toc464802509)

[Information System Name/Title 351](#_Toc464802510)

[E-Authentication Level Definitions 351](#_Toc464802511)

[Review Maximum Potential Impact Levels 352](#_Toc464802512)

[E-Authentication Level Selection 352](#_Toc464802513)

[ATTACHMENT 4 – PTA / PIA 354](#_Toc464802514)

[Privacy Overview and Point of Contact (POC) 354](#_Toc464802515)

[Applicable Laws and Regulations 354](#_Toc464802516)

[Applicable Standards and Guidance 355](#_Toc464802517)

[Personally Identifiable Information (PII) 355](#_Toc464802518)

[Privacy Threshold Analysis 356](#_Toc464802519)

[Qualifying Questions 356](#_Toc464802520)

[Designation 356](#_Toc464802521)

[ATTACHMENT 5 - Rules of Behavior 357](#_Toc464802522)

[ATTACHMENT 6 – Information System Contingency Plan 358](#_Toc464802523)

[ATTACHMENT 7 - Configuration Management Plan 359](#_Toc464802524)

[ATTACHMENT 8 - Incident Response Plan 360](#_Toc464802525)

[ATTACHMENT 9 - CIS Report and Worksheet 361](#_Toc464802526)

[ATTACHMENT 10 - FIPS 199 362](#_Toc464802527)

[Introduction and Purpose 362](#_Toc464802528)

[Scope 362](#_Toc464802529)

[System Description 362](#_Toc464802530)

[Methodology 363](#_Toc464802531)

[ATTACHMENT 11 - Separation of Duties Matrix 365](#_Toc464802532)

[ATTACHMENT 12 – FedRAMP Laws and Regulations 366](#_Toc464802533)

[ATTACHMENT 13 – FedRAMP Inventory Workbook 367](#_Toc464802534)

List of Tables

[Table 1‑1 Information System Name and Title 1](#_Toc462729295)

[Table 2‑1 Security Categorization 1](#_Toc462729296)

[Table 2‑2 Sensitivity Categorization of Information Types 3](#_Toc462729297)

[Table 2‑3 Security Impact Level 3](#_Toc462729298)

[Table 2‑4 Baseline Security Configuration 3](#_Toc462729299)

[Table 3‑1 Information System Owner 4](#_Toc462729300)

[Table 5‑1 Information System Management Point of Contact 5](#_Toc462729301)

[Table 5‑2 Information System Technical Point of Contact 5](#_Toc462729302)

[Table 6‑1 CSP Name Internal ISSO (or Equivalent) Point of Contact 6](#_Toc462729303)

[Table 6‑2 AO ISSO Point of Contact 6](#_Toc462729304)

[Table 7‑1 System Status 6](#_Toc462729305)

[Table 8‑1 Service Layers Represented in this SSP 7](#_Toc462729306)

[Table 8‑2 Cloud Deployment Model Represented in this SSP 8](#_Toc462729307)

[Table 8‑3 Leveraged Authorizations 8](#_Toc462729308)

[Table 9‑1 Personnel Roles and Privileges 10](#_Toc462729309)

[Table 10‑1 Ports, Protocols and Services 14](#_Toc462729310)

[Table 11‑1 System Interconnections 15](#_Toc462729311)

[Table 12‑1 Information System Name Laws and Regulations 16](#_Toc462729312)

[Table 12‑2 Information System Name Standards and Guidance 16](#_Toc462729313)

[Table 13‑1 Summary of Required Security Controls 17](#_Toc462729314)

[Table 13‑2 Control Origination and Definitions 25](#_Toc462729315)

[Table 13‑3 CA-3 Authorized Connections 100](#_Toc462729316)

[Table 15‑1. Attachment File Naming Convention 348](#_Toc462729317)

List of Figures

[Figure 9‑1 Authorization Boundary Diagram 9](#_Toc462729318)

[Figure 9‑2 Network Diagram 11](#_Toc462729319)

[Figure 10‑1 Data Flow Diagram 13](#_Toc462729320)

System Security Plan Approvals

Cloud Service Provider Signatures

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | | | |
| Name | <Enter Name> | | Date | <Select Date> |
| Title | <Enter Title> | | | |
| Cloud Service Provider | | CSP Name | | |
|  | | | | |
|  | | | | |
|  | | | | |
| Name | <Enter Name> | | Date | <Select Date> |
| Title | <Enter Title> | | | |
| Cloud Service Provider | | CSP Name | | |
|  | | | | |
|  | | | | |
|  | | | | |
| Name | <Enter Name> | | Date | <Select Date> |
| Title | <Enter Title> | | | |
| Cloud Service Provider | | CSP Name | | |
|  | |  | | |

# Information System Name/Title

This System Security Plan provides an overview of the security requirements for the Information System Name (Information System Abbreviation) 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 Information System Abbreviation information system.

The security safeguards implemented for the Information System Abbreviation 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 ‑ Information System Name and Title

| Unique Identifier | Information System Name | Information System Abbreviation |
| --- | --- | --- |
| <Enter FedRAMP Application Number> | Information System Name | Information System Abbreviation |

# 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 ‑ Security Categorization

|  |  |
| --- | --- |
| System Sensitivity Level: | Choose level. |

## 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 Information System Abbreviation. The selection of the information types is based on guidance provided by 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.

Instruction: Record your information types in the tables that follow. Record the sensitivity level for Confidentiality, Integrity and Availability as High, Moderate, or Low. Add more rows as needed to add more information types. Use NIST SP 800-60 Guide for Mapping Types of Information and Systems to Security Categories, Volumes I & II, Revision 1 for guidance.

Delete this instruction from your final version of this document.

Example:

| 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 Development | C.3.5.1 | Low | Moderate | Low |

Table ‑ 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 |
| --- | --- | --- | --- | --- |
| <Enter Information Type> | <Enter NIST Identifier> | Choose level. | Choose level. | Choose level. |
| <Enter Information Type> | <Enter NIST Identifier> | Choose level. | Choose level. | Choose level. |
| <Enter Information Type> | <Enter NIST Identifier> | Choose level. | Choose level. | Choose level. |

## Security Objectives Categorization (FIPS 199)

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

Table ‑ Security Impact Level

| Security Objective | Low, Moderate or High |
| --- | --- |
| Confidentiality | Choose level. |
| Integrity | Choose level. |
| Availability | Choose level. |

Through review and analysis it has been determined that the baseline security categorization for the Information System Abbreviation system is listed in the Table 2‑4 Baseline Security Configuration that follows.

Table ‑ Baseline Security Configuration

|  |  |
| --- | --- |
| Information System Abbreviation Security Categorization | Choose level |

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.

## E-Authentication Determination

The e-Authentication information may be found in section: ATTACHMENT 3 – e-Authentication Worksheet

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 Choose an item.

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

# Information System Owner

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

Table ‑ Information System Owner

| Information System Owner Information | |
| --- | --- |
| Name | <Enter Name> |
| Title | <Enter Title> |
| Company / Organization | <Enter Company/Organization>. |
| Address | <Enter Address, City, State and Zip> |
| Phone Number | <555-555-5555> |
| Email Address | <Enter email address> |

# Authorizing Official

Instruction: The Authorizing Official is determined by the path that the CSP is using to obtain an authorization.

JAB P-ATO: FedRAMP, JAB, as comprised of member representatives from the General Services Administration (GSA), Department of Defense (DoD) and Department of Homeland Security (DHS)

Agency Authority to Operate (ATO): Agency Authorizing Official name, title and contact information

Delete this and all other instructions from your final version of this document.

The Authorizing Official (AO) or Designated Approving Authority (DAA) for this information system is the Insert AO information as instructed above.

# Other Designated Contacts

Instruction: AOs should use the following section to identify points of contact that understand the technical implementations of the identified cloud system. AOs should edit, add, or modify the contacts in this section as they see fit.

Delete this and all other instructions from your final version of this document.

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

Table ‑ Information System Management Point of Contact

| Information System Management Point of Contact | |
| --- | --- |
| Name | <Enter Name> |
| Title | <Enter Title> |
| Company / Organization | <Enter Company/Organization>. |
| Address | <Enter Address, City, State and Zip> |
| Phone Number | <555-555-5555> |
| Email Address | <Enter email address> |

Table ‑ Information System Technical Point of Contact

| Information System Technical Point of Contact | |
| --- | --- |
| Name | <Enter Name> |
| Title | <Enter Title> |
| Company / Organization | <Enter Company/Organization>. |
| Address | <Enter Address, City, State and Zip> |
| Phone Number | <555-555-5555> |
| Email Address | <Enter email address> |

Instruction: Add more tables as needed.

Delete this and all other instructions from your final version of this document.

| Point of Contact | |
| --- | --- |
| Name | <Enter Name> |
| Title | <Enter Title> |
| Company / Organization | <Enter Company/Organization>. |
| Address | <Enter Address, City, State and Zip> |
| Phone Number | <555-555-5555> |
| Email Address | <Enter email address> |

# 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 ‑ CSP Name Internal ISSO (or Equivalent) Point of Contact

| CSP Name Internal ISSO (or Equivalent) Point of Contact | |
| --- | --- |
| Name | <Enter Name> |
| Title | <Enter Title> |
| Company / Organization | <Enter Company/Organization>. |
| Address | <Enter Address, City, State and Zip> |
| Phone Number | <555-555-5555> |
| Email Address | <Enter email address> |

Table ‑ AO ISSO Point of Contact

|  |  |
| --- | --- |
| AO ISSO Point of Contact | |
| Name | <Enter Name> |
| Title | ISSO |
| Organization | <Enter Company/Organization>. |
| Address | <Enter Address, City, State and Zip> |
| Phone Number | <555-555-5555> |
| Email Address | <Enter email address> |

# 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 ‑ 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: Click here to enter text. |

Instruction: Select as many status indicators as apply. If more than one status is selected, list which components of the system are covered under each status indicator.

Delete this and all other instructions from your final version of this document.

# Information System Type

The Information System Abbreviation makes use of unique managed service provider architecture layer(s).

## 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 an 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 an SaaS. A no response means that the system is either a PaaS or an IaaS. |

The layers of the Information System Abbreviation defined in this SSP are indicated in Table 8‑1 Service Layers Represented in this SSP that follows.

Instruction: Check all layers that apply.

Delete this and all other instructions from your final version of this document.

Table ‑ 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: Click here to enter text. |

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

## Cloud Deployment Models

Information systems are made up of different deployment models. The deployment models of the Information System Abbreviation 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.

Instruction: Check deployment model that applies.

Delete this and all other instructions from your final version of this document.

Table ‑ 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)  Click here to enter text. |

## Leveraged Authorizations

Instruction: The FedRAMP program qualifies different service layers for Authorizations. One or multiple service layers can be qualified in one System Security Plan. See the section on Use Cases in Guide to Understanding FedRAMP for more information. If a lower level layer has been granted an Authorization and another higher level layer represented by this SSP plans to leverage a lower layer’s Authorization, this System Security Plan must clearly state that intention. If an information system does not leverage any pre-existing Authorizations, write “None” in the first column of the table that follows. Add as many rows as necessary in the table that follows.

Delete this and all other instructions from your final version of this document.

The Information System Abbreviation Choose an item leverages a pre-existing FedRAMP Authorization. FedRAMP Authorizations leveraged by this Information System Abbreviation are listed in Table 8‑3 Leveraged Authorizations that follows.

Table ‑ Leveraged Authorizations

| Leveraged Information System Name | Leveraged Service Provider Owner | Date Granted |
| --- | --- | --- |
| <Enter Leveraged information system name1> | <Enter service provider owner1> | <Date> |
| <Enter Leveraged information system name2> | <Enter service provider owner2> | <Date> |
| <Enter Leveraged information system name3> | <Enter service provider owner3> | <Date> |

# General System Description

This section includes a general description of the Information System Abbreviation.

## System Function or Purpose

Instruction: In the space that follows, describe the purpose and functions of this system.

Delete this and all other instructions from your final version of this document.

## Information System Components and Boundaries

Instruction: In the space that follows, provide an explicit definition of the system’s Authorization Boundary. Provide a diagram that portrays this Authorization Boundary and all its connections and components, including the means for monitoring and controlling communications at the external boundary and at key internal boundaries within the system.

Address all components and managed interfaces of the information system authorized for operation (e.g., routers, firewalls).

Formal names of components as they are known at the service provider organization in functional specifications, configuration guides, other documents and live configurations shall be named on the diagram and described. Components identified in the Boundary diagram should be consistent with the Network diagram and the inventory(ies). Provide a key to symbols used. Ensure consistency between the boundary and network diagrams and respective descriptions (Section 9.4) and the appropriate Security Controls [AC-20, CA-3(1)]. See the Guide to Understanding FedRAMP for more information.

Delete this and all other instructions from your final version of this document.

A detailed and explicit definition of the system authorization boundary diagram is represented in Figure 9‑1 Authorization Boundary Diagram below.

|  |
| --- |
|  |

Figure ‑ Authorization Boundary Diagram

## 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.

Instruction: For an External User, write “Not Applicable” in the Sensitivity Level Column. This table must include all roles including systems administrators and database administrators as a role types. (Also include web server administrators, network administrators and firewall administrators if these individuals have the ability to configure a device or host that could impact the CSP service offering.)

This table must also include whether these roles are fulfilled by foreign nationals or systems outside the United States.

Delete this and all other instructions from your final version of this document.

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 |
| --- | --- | --- | --- | --- | --- |
| UNIX System Administrator | Internal | P | Moderate | Full administrative access (root) | Add/remove users and hardware, install and configure software, OS updates, patches and hotfixes, perform backups |
| Client Administrator | External | NP | N/A | Portal administration | Add/remote client users. Create, modify and delete client applications |
| Program Director | Internal | NLA | Limited | N/A | Reviews, approves and enforces policy |
|  | Choose an item. | Choose an item. | Choose an item. |  |  |
|  | Choose an item. | Choose an item. | Choose an item. |  |  |
|  | Choose an item. | Choose an item. | Choose an item. |  |  |
|  | Choose an item. | Choose an item. | Choose an item. |  |  |

There are currently <number> internal personnel and <number> external personnel. Within one year, it is anticipated that there will be <number> internal personnel and <number> external personnel.

## Network Architecture

Instruction: Insert a network architectural diagram in the space that follows. Ensure that the following items are labeled on the diagram: hostnames, Domain Name System (DNS) servers, DHCP servers, authentication and access control servers, directory servers, firewalls, routers, switches, database servers, major applications, storage, Internet connectivity providers, telecom circuit numbers, network interfaces and numbers, VLANs. Major security components should be represented. If necessary, include multiple network diagrams.

Delete this and all other instructions from your final version of this document.

Assessors should be able to easily map hardware, software and network inventories back to this diagram.

The logical network topology is shown in Figure 9‑2 Network Diagram mapping the data flow between components.

The following Figure 9‑2 Network Diagram(s) provides a visual depiction of the system network components that constitute Information System Abbreviation.

|  |
| --- |
|  |

Figure ‑ Network Diagram

# System Environment And Inventory

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

Instruction: In the space that follows, provide a general description of the technical system environment. Include information about all system environments that are used, e.g., production environment, test environment, staging or QA environments. Include the specific location of the alternate, backup and operational facilities.

In your description, also include a reference to Attachment 13, the system’s Integrated Inventory Workbook, which should provide a complete listing of the system’s components (operating systems/infrastructure, web applications/software, and databases). The Integrated Inventory Workbook should be maintained and updated monthly by the CSP, as part of continuous monitoring efforts. Instructions for completing the Integrated Inventory Workbook are provided within the Integrated Inventory Workbook.

Delete this and all other instructions from your final version of this document.

## Data Flow

Instruction: In the space that follows, describe the flow of data in and out of system boundaries and insert a data flow diagram. Describe protections implemented at all entry and exit points in the data flow as well as internal controls between customer and project users. See Guide to Understanding FedRAMP for a dataflow example. If necessary, include multiple data flow diagrams.

Delete this and all other instructions from your final version of this document.

The data flow in and out of the system boundaries is represented in Figure 10‑1 Data Flow Diagram below.

|  |
| --- |
|  |

Figure ‑ Data Flow Diagram

## Ports, Protocols and Services

The Table 10‑1 Ports, Protocols and Services below lists the ports, protocols and services enabled in this information system.

Instruction: In the column labeled “Used By” please indicate the components of the information system that make use of the ports, protocols and services. In the column labeled “Purpose” indicate the purpose for the service (e.g., system logging, HTTP redirector, load balancing). This table should be consistent with CM-6 and CM-7. You must fill out this table, even if you are leveraging a pre-existing FedRAMP Authorization. Add more rows as needed.

Delete this and all other instructions from your final version of this document.

Table ‑ Ports, Protocols and Services

| Ports (TCP/UDP)\* | Protocols | Services | Purpose | Used By |
| --- | --- | --- | --- | --- |
| <Enter Port> | <Enter Protocols> | <Enter Services> | <Enter Purpose> | <Enter Used By> |
| <Enter Port> | <Enter Protocols> | <Enter Services> | <Enter Purpose> | <Enter Used By> |
| <Enter Port> | <Enter Protocols> | <Enter Services> | <Enter Purpose> | <Enter Used By> |
| <Enter Port> | <Enter Protocols> | <Enter Services> | <Enter Purpose> | <Enter Used By> |
| <Enter Port> | <Enter Protocols> | <Enter Services> | <Enter Purpose> | <Enter Used By> |
| <Enter Port> | <Enter Protocols> | <Enter Services> | <Enter Purpose> | <Enter Used By> |

\* Transmission Control Protocol (TCP), User Diagram Protocol (UDP)

# System Interconnections

Instruction: List all interconnected systems. Provide the IP address and interface identifier (eth0, eth1, eth2) for the CSP system that provides the connection. Name the external organization and the IP address of the external system. Indicate how the connection is being secured. For Connection Security indicate how the connection is being secured. For Data Direction, indicate which direction the packets are flowing. For Information Being Transmitted, describe what type of data is being transmitted. If a dedicated telecom line is used, indicate the circuit number. Add additional rows as needed. This table must be consistent with Table 13‑3 CA-3 Authorized Connections.

Delete this and all other instructions from your final version of this document.

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

Table ‑ System Interconnections

| SP\* IP Address and Interface | External Organization Name and IP Address of System | External Point of Contact and Phone Number | Connection Security (IPSec VPN, SSL, Certificates, Secure File Transfer, etc.)\*\* | Data Direction  (incoming, outgoing, or both) | Information Being Transmitted | Port or Circuit Numbers |
| --- | --- | --- | --- | --- | --- | --- |
| <SP IP Address/Interface> | <External Org/IP> | <External Org POC>  <Phone 555-555-5555> | <Enter Connection Security> | Choose an item. | <Information Transmitted> | <Port/Circuit Numbers> |
| <SP IP Address/Interface> | <External Org/IP> | <External Org POC>  <Phone 555-555-5555> | <Enter Connection Security> | Choose an item. | <Information Transmitted> | <Port/Circuit Numbers> |
| <SP IP Address/Interface> | <External Org/IP> | <External Org POC>  <Phone 555-555-5555> | <Enter Connection Security> | Choose an item. | <Information Transmitted> | <Port/Circuit Numbers> |
| <SP IP Address/Interface> | <External Org/IP> | <External Org POC>  <Phone 555-555-5555> | <Enter Connection Security> | Choose an item. | <Information Transmitted> | <Port/Circuit Numbers> |
| <SP IP Address/Interface> | <External Org/IP> | <External Org POC>  <Phone 555-555-5555> | <Enter Connection Security> | Choose an item. | <Information Transmitted> | <Port/Circuit Numbers> |
| <SP IP Address/Interface> | <External Org/IP> | <External Org POC>  <Phone 555-555-5555> | <Enter Connection Security> | Choose an item. | <Information Transmitted> | <Port/Circuit Numbers> |

\*Service Processor

\*\*Internet Protocol Security (IPSec), Virtual Private Network (VPN), Secure Sockets Layer (SSL)

# Laws, Regulations, Standards and Guidance

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

## 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 Information System Name Laws and Regulations includes additional laws and regulations specific to Information System Name.

Instruction: The information system name is a repeatable field that is populated when the Title Page is completed. If the CSP does not have additional laws and regulations that it must follow, please specify "N/A" in the table.

Delete this and all other instructions from your final version of this document.

Table ‑ Information System Name Laws and Regulations

|  |  |  |  |
| --- | --- | --- | --- |
| Identification Number | Title | Date | Link |
| <Reference ID> | <Reference Title> | <Ref Date> | <Reference Link> |
| <Reference ID> | <Reference Title> | <Ref Date> | <Reference Link> |
| <Reference ID> | <Reference Title> | <Ref Date> | <Reference Link> |

## 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 Information System Name Standards and Guidance includes in this section any additional standards and guidance specific to Information System Name.

Instruction: The information system name is a repeatable field that is populated when the Title Page is completed. If the CSP does not have additional standards or guidance that it must follow, please specify "N/A" in the table.

Delete this and all other instructions from your final version of this document.

Table ‑ Information System Name Standards and Guidance

|  |  |  |  |
| --- | --- | --- | --- |
| Identification Number | Title | Date | Link |
| <Reference ID> | <Reference Title> | <Ref Date> | <Reference Link> |
| <Reference ID> | <Reference Title> | <Ref Date> | <Reference Link> |
| <Reference ID> | <Reference Title> | <Ref Date> | <Reference Link> |

# 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 Information System Abbreviation 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 ‑ 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: The -1 Controls (AC-1, AU-1, SC-1, etc.) cannot be inherited and must be provided in some way by the service provider.

Instruction: In the sections that follow, describe the information security control as it is implemented on the system. All controls originate from a system or from a business process. It is important to describe where the control originates from so that it is clear whose responsibility it is to implement, manage and monitor the control. In some cases, the responsibility is shared by a CSP and by the customer. Use the definitions in the table that follows to indicate where each security control originates from. 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)

Throughout this SSP, policies and procedures must be explicitly referenced (title and date or version) so that it is clear which document is being referred to. Section numbers or similar mechanisms should allow the reviewer to easily find the reference.

For Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) and Software as a Service (SaaS) systems that are inheriting controls from Microsoft Azure, the “inherited” check box must be checked and the implementation description must simply say “inherited.” FedRAMP reviewers will determine whether the control-set is appropriate or not.

For some controls, the JAB has chosen to define or provide parameters, in others they have left the decision up to the organization. The FedRAMP assignments and customer-defined selections and assignments are listed in the parameters of each control summary information section.

Delete this and all other instructions from your final version of this document.

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

Table ‑ Control Origination and Definitions

| Control Origination | Definition | Example |
| --- | --- | --- |
| Service Provider Corporate | A control that originates from the CSP Name 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 CSP Name 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 CSP Name. | 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 CSP Name 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 CSP Name system that has already received a FedRAMP Authorization. | A PaaS or SaaS provider inherits PE controls from an IaaS provider. |

\*Hyper Text Transport Protocol (http)

Responsible Role indicates the role of CSP employee who can best respond to questions about the particular control that is described.

## Access Control (AC)

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

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:

* 1. Access control policy [FedRAMP Assignment: at least annually]; and

Access control procedures [FedRAMP Assignment: at least annually or whenever a significant change occurs].

| AC-1 | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer-defined*> | |
| Parameter AC-1(a): <*Customer-defined personnel or roles*> | |
| Parameter AC-1(b)(1): <*FedRAMP Assignment: at least annually*> | |
| Parameter AC-1(b)(2): <*FedRAMP Assignment: at least annually or whenever a significant change occurs*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| AC-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for developing, documenting, reviewing, updating, and disseminating the access control policy and procedures. The customer access control policy and procedures address access to all customer-deployed resources and customer system access (e.g., access to customer-deployed virtual machines, access to customer-built applications). The customer implementation statement should address the content of the policy (which must include purpose, scope, roles, responsibilities, management commitment, coordination, and compliance), procedures (which must facilitate the implementation of the policies and associated controls), frequency of review, and the role(s) responsible. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for developing, documenting, reviewing, updating, and disseminating the access control policy and procedures. The customer access control policy and procedures address access to all customer-deployed resources and customer system access (e.g., access to customer-deployed virtual machines, access to customer-built applications). The customer implementation statement should address the content of the policy (which must include purpose, scope, roles, responsibilities, management commitment, coordination, and compliance), procedures (which must facilitate the implementation of the policies and associated controls), frequency of review, and the role(s) responsible. |

### AC-2 Account Management (H)

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: monthly for privileged accessed, every six (6) months for non-privileged access]; and
11. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

| AC-2 | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer-defined*> | |
| Parameter AC-2(a): <*Customer-defined account types*> | |
| Parameter AC-2(e): <*Customer-defined personnel or roles*> | |
| Parameter AC-2(f): <*Customer-defined procedures or conditions*> | |
| Parameter AC-2(j): <*FedRAMP Assignment: monthly for privileged accessed, every six (6) months for non-privileged access*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (PaaS)**  The customer is responsible for identifying all customer-controlled accounts within the system. The customer control implementation statement should address all account types within the system in use and how each type supports a mission/business function. Example account types may include, but are not limited to: Azure Active Directory individual user accounts (used to manage access to Azure resources), database, shared server admin accounts, application-level individual user accounts.  **Customer Responsibility (IaaS)**  The customer is responsible for identifying all customer-controlled accounts within the system. The customer control implementation statement should address all account types within the system in use and how each type supports a mission/business function. Example account types may include, but are not limited to: Azure Active Directory individual user accounts (used to manage access to Azure resources), operating system-level individual user accounts for IaaS virtual machines, database, shared server admin accounts, application-level individual user accounts. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for assigning managers to the accounts identified in AC-02.a. The customer control implementation statement should address how account managers are identified within the organization. |
| Part c | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for establishing role and group membership criteria for customer-controlled account types (see AC-02.a). The customer control implementation statement should address the criteria defined for group and role membership. |
| Part d | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for establishing an authorization process for all customer-controlled account types (see AC-02.a). The customer control implementation statement should address the process by which authorized users are specified and privilege levels are determined. |
| Part e | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for requiring personnel to approve the creation of new accounts for the system. The customer control implementation statement should address the personnel or roles designated to approve all customer-controlled account types (see AC-02.a). |
| Part f | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for establishing an account management process for all customer-controlled account types (see AC-02.a). The customer control implementation statement should address the account management process lifecycle from creation to disablement/removal. |
| Part g | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for monitoring the use of all customer-controlled accounts. The customer control implementation statement should address how the customer monitors account use, including the personnel or roles responsible for monitoring activities. |
| Part h | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for notifying account managers (defined in AC-02.b) of all customer-controlled accounts when users are terminated or transferred, accounts are no longer required, or system usage or need-to-know changes. The customer control implementation statement should address the methods by which these triggering events are identified and the managers are notified. |
| Part i | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for authorizing access to the customer system. The customer control implementation statement should address the requirement that all system access is granted based on a valid authorization for a specific intended usage. |
| Part j | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for reviewing customer-controlled accounts at the required frequency to determine if accounts are compliant with all organization requirements. The customer control implementation statement should address the process used to review account compliance. |
| Part k | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for the management of customer-controlled shared/group account credentials when a user is removed from the shared/group account. The customer control implementation statement should address the process for reissuing shared/group account credentials when users are removed from that shared/group account. |

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

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

| AC-2(1) | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer-defined*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-2 (1) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for employing automated mechanisms to support account management activities for the account types defined in AC-02.a. The customer control implementation statement should address the automated mechanisms put in place for account management. |

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

The information system automatically [FedRAMP Selection: disables] temporary and emergency accounts after [FedRAMP Assignment: 24 hours from last use].

| AC-2 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer-defined*> | |
| Parameter AC-2(2)1: *<FedRAMP Selection: disables>* | |
| Parameter AC-2(2)2: <*FedRAMP Assignment: 24 hours from last use*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-2 (2) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for configuring the system to automatically remove or disable emergency and temporary accounts, if those accounts have been defined in AC-02.a. The customer control implementation statement should address the selection of removal or disablement of temporary and emergency accounts, and the time period during which those accounts are allowed to remain active before removal/disablement. |

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

The information system automatically disables inactive accounts after [FedRAMP Assignment: thirty-five (35) 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 JAB/AO. Where user management is a function of the service, reports of activity of consumer users shall be made available.

|  |  |
| --- | --- |
| AC-2 (3) | Control Enhancement Summary Information |
| Responsible Role: <*Customer-defined*> | |
| Parameter AC-2(3): <*FedRAMP Assignment: thirty-five (35) days for user accounts*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-2 (3) What is the solution and how is it implemented |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for configuring the system to automatically disable user accounts (for account types identified in AC-02.a) after an organization-defined period of inactivity. The customer control implementation statement should address the automated mechanisms involved in disabling inactive accounts, and the time period during which those accounts are allowed to remain inactive before disablement. |

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

The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies [FedRAMP Assignment: organization and/or service provider system owner].

| AC-2 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer-defined*> | |
| Parameter AC-2(4): *<FedRAMP Assignment: organization and/or service provider system owner>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-2 (4) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for implementing an automated audit and notification system for the lifecycle of managing customer-controlled accounts. The customer control implementation statement should address how account changes will be audited and the personnel/roles notified. |

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

The organization requires that users log out when [FedRAMP Assignment: inactivity is anticipated to exceed fifteen (15) minutes].

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

Guidance: Should use a shorter timeframe than AC-12

| AC-2 (5) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter AC-2(5): *<FedRAMP Assignment: inactivity is anticipated to exceed fifteen (15) minutes>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-2 (5) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for enforcing an inactivity log out policy. The customer control implementation statement should address the period of inactivity and/or the description of when to log out. |

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

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 [FedRAMP Assignment: disables//revokes access within an organization-specified timeframe] when privileged role assignments are no longer appropriate.

| AC-2 (7) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter AC-2(7)(c): <*FedRAMP Assignment: disables//revokes access within an organization-specified timeframe*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-2 (7) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for administering privileged user accounts using a role based access scheme (for customer-controlled accounts). The customer control implementation statement should address the organizations role-based access scheme and how it is used to establish and administer privileged user accounts. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for monitoring privileged roles of customer-controlled accounts. The customer control implementation statement should address the mechanisms used for monitoring privileged role assignments. |
| Part c | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for taking action on customer-controlled accounts when privileged role assignments are no longer appropriate. The customer control implementation statement should address the actions to be taken when a user no longer requires a privileged role. |

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

The organization only permits the use of shared/group accounts that meet [FedRAMP Assignment: organization-defined need with justification statement that explains why such accounts are necessary].

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

| AC-2 (9) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter AC-2(9): <*FedRAMP Assignment: organization-defined need with justification statement that explains why such accounts are necessary*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-2 (9) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for restricting the use of customer-controlled shared/group accounts. The customer control implementation statement should address the organizations specific requirements for the establishment of a shared/group 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-2 (10) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-2 (10) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for the termination of customer-controlled shared/group account credentials. The customer control implementation statement should address the process for terminating shared/group credentials when a member leaves. |

#### AC-2 (11) Control Enhancement (H)

The information system enforces [Assignment: organization-defined circumstances and/or usage conditions] for [Assignment: organization-defined information system accounts].

| AC-2 (11) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter AC-2 (11)-1: *<Customer-defined circumstances or usage conditions>* | |
| Parameter AC-2 (11)-2: *<Customer-defined accounts>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-2 (11) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for enforcing the appropriate usage of all customer-controlled accounts within the system. The customer control implementation statement should address the accounts used within the system and the intended use of those accounts. |

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

The organization:

1. Monitors information system accounts for [Assignment: organization-defined atypical use]; and
2. Reports atypical usage of information system accounts to [FedRAMP Assignment: at a minimum, the ISSO and/or similar role within the organization].

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

| AC-2 (12) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer defined>* | |
| Parameter AC-2(12)(a): <*Customer-defined atypical use*> | |
| Parameter AC-2(12)(b): *<FedRAMP Assignment: at a minimum, the ISSO and/or similar role within the organization>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-2 (12) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for monitoring customer-controlled accounts for atypical usage. The customer control implementation statement should address the criteria defining atypical account behavior, and the mechanisms used to monitor that criteria. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for reporting atypical behavior of customer-controlled accounts. The customer control implementation statement should address which personnel/roles will be notified when atypical account behavior occurs. |

#### AC-2 (13) Control Enhancement (H)

The organization disables accounts of users posing a significant risk within [FedRAMP Assignment: one (1) hour] of discovery of the risk.

| AC-2 (13) | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer-defined*> | |
| Parameter AC-2 (13): *<FedRAMP Assignment: one hour>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-2 (13) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for disabling customer-controlled accounts of users posing a significant risk. The customer control implementation statement should address the process for disabling high-risk user accounts and the time period in which disablement must occur. |

### 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-3 | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-3 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for enforcing approved authorizations for logical access to customer-deployed resources. The customer control implementation statement should address the processes and/or mechanisms used to enforce the authorization to access system resources. |

### 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-4 | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter AC-4: *<Customer-defined information flow control 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-4 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for controlling the flow of information within customer-deployed resources and between interconnected systems. The customer control implementation statement should address the customer’s information flow control policies and enforcement mechanisms. |

#### AC-4 (8) Control Enhancement (H)

The information system enforces information flow control using [Assignment: organization-defined security policy filters] as a basis for flow control decisions for [Assignment: organization-defined information flows].

| AC-4 (8) | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer-defined*> | |
| Parameter AC-4 (8)-1: *<FedRAMP Assignment: security policy filters>* | |
| Parameter AC-4 (8)-2: *<FedRAMP Assignment: organization-defined information flows>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-4 (8) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for enforcing information flow control within customer-deployed resources. The customer control implementation statement should address the security policy filters in place to enforce information flow control policies. |

#### 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-4 (21) | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer-defined*> | |
| Parameter AC-4(21)-1: *<Customer-defined mechanisms and/or techniques>* | |
| Parameter AC-4(21)-2: *<Customer-defined required separations by types of 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-4 (21) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for separating information flows within customer-deployed resources. The customer control implementation statement should address the separations required by information type, and the mechanisms and/or techniques used to separate information flows. |

### 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 0 ATTACHMENT 11 - Separation of Duties Matrix.

| AC-5 | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter AC-5(a): *<Customer-defined duties of individuals>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for the separation of duties across customer-controlled accounts. The customer control implementation statement should address how individual duties are defined and separated. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for documenting the separation of duties across customer-controlled accounts. The customer control implementation statement should address which duties require separation and how they are separated. |
| Part c | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for defining system access authorizations to support separation of duties across customer-controlled accounts. The customer control implementation statement should address the mechanisms in place to enforce the separation of duties. |

### 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-6 | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-6 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for enforcing least privilege across customer-controlled accounts. The customer control implementation statement should address the level of access required to perform each job function, and how the role based access control scheme enforces least privilege based upon organization requirements. |

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

The organization explicitly authorizes access to [FedRAMP Assignment: all functions not publicly accessible and all security-relevant information not publicly available].

| AC-6 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: <Customer-defined> | |
| Parameter AC-6(1): *<FedRAMP Assignment: all functions not publicly accessible and all security-relevant information not publicly available>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-6 (1) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for authorizing access to security functions for customer-controlled accounts. The customer control implementation statement should address criteria used to determine which security functions and information require explicit access authorization. |

#### 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-6 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: <Customer-defined> | |
| Parameter AC-6(2): *<FedRAMP Assignment: 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 FedRAMP Authorization for Date of Authorization , | |

| AC-6 (2) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for requiring the use of non-privileged accounts/roles when accessing non-security functions for customer-deployed resources. The customer control implementation statement should address the user account/roles that have privileged access to organization-defined security functions and/or security-relevant information, and the requirement that those users leverage non-privileged accounts/roles when accessing non-security functions or information. |

#### AC-6 (3) Control Enhancement (H)

The organization authorizes network access to [FedRAMP Assignment: all privileged commands] only for [Assignment: organization-defined compelling operational needs] and documents the rationale for such access in the security plan for the information system.

| AC-6 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter AC-6 (3)-1: *<FedRAMP Assignment: all privileged commands>* | |
| Parameter AC-6 (3)-2: *<Customer-defined compelling operational needs>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-6 (3) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for enforcing least privilege when authorizing network access to privileged commands for customer-deployed resources. The customer control implementation statement should address privileged commands and their operational need, and document the rationale for access in the system security plan (SSP). |

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

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

| AC-6 (5) | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer-defined>* | |
| Parameter AC-6 (5): *<Customer-defined personnel or roles>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-6 (5) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for restricting privileged customer-controlled accounts. The customer control implementation statement should address the personnel/roles which require privileged system access. |

#### AC-6 (7) Control Enhancement (H)

The organization:

1. Reviews [FedRAMP Assignment: at a minimum, annually] the privileges assigned to [FedRAMP Assignment: all users with privileges] to validate the need for such privileges; and

Reassigns or removes privileges, if necessary, to correctly reflect organizational mission/business needs.

| AC-6 (7) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter AC-6(7)(a)-1: *<FedRAMP Assignment: at a minimum, annually>* | |
| Parameter AC-6(7)(a)-2: *<FedRAMP Assignment: all users with privileges>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-6 (7) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for reviewing user privileges of customer-controlled accounts. The customer control implementation statement should address the frequency of reviews and the roles/classes requiring review. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for reassigning or removing privileges for customer-controlled accounts when appropriate. The customer control implementation statement should address the actions taken when user privileges are found to be inappropriate. |

#### AC-6 (8) Control Enhancement (H)

The information system prevents [FedRAMP Assignment: any software except software explicitly documented] from executing at higher privilege levels than users executing the software.

| AC-6 (8) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter AC-6 (8): *<FedRAMP Assignment: any software except software explicitly documented>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-6 (8) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for enforcing software execution privileges on customer-deployed resources. The customer control implementation statement should address the mechanisms in place to prevent software from executing at a higher level than that of its user. |

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

The information system audits the execution of privileged functions.

| AC-6 (9) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-6 (9) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for auditing the execution of privileged functions on customer-deployed resources. The customer control implementation statement should address privileged functions and the mechanisms in place to audit their execution. |

#### 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-6 (10) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-6 (10) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for ensuring that non-privileged users cannot execute privileged functions on customer-deployed resources. The customer control implementation statement should address the mechanisms in place preventing non-privileged users from executing privileged functions. |

### AC-7 Unsuccessful Login Attempts (H)

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: minimum of three (3) hours or until unlocked by an administrator]; delays next logon prompt according to [Assignment: organization-defined delay algorithm]] when the maximum number of unsuccessful attempts is exceeded.

| AC-7 | Control Summary Information |
| --- | --- |
| Responsible Role: <Customer-defined> | |
| Parameter AC-7(a)-1: *<FedRAMP Assignment: not more than three (3)>* | |
| Parameter AC-7(a)-2: *<FedRAMP Assignment: fifteen (15) minutes>* | |
| Parameter AC-7(b)-1: *<FedRAMP Assignment: minimum of three (3) hours or until unlocked by an administrator>* | |
| Parameter AC-7(b)-2: *<Customer-defined delay algorithm>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-7 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for enforcing a limit of consecutive failed login attempts on customer-deployed resources. The customer control implementation statement should address the number of failed login attempts allowed and the time period within which those attempts can occur. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for taking action when a user has reached the number of failed login attempts within the time period documented in AC-07.a. The customer control implementation statement should address which actions the system takes when the requirements of AC-07.a have been exceeded. |

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

The information system purges/wipes information from [FedRAMP Assignment: mobile devices as defined by organization policy] based on [Assignment: organization-defined purging/wiping requirements/techniques] after [FedRAMP Assignment: three (3)] consecutive, unsuccessful device logon attempts.

| AC-7 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: Not Applicable | |
| Parameter AC-7 (2)-1: Not Applicable | |
| Parameter AC-7 (2)-2: Not Applicable | |
| Parameter AC-7 (2)-3: 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-7 (2) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure does not allow mobile devices within the Azure boundary. As such, this control is not applicable to Microsoft Azure.  **Customer Responsibility (IaaS/PaaS)**  There are no customer-controlled mobile devices within the scope of systems deployed on Azure; all mobile device protection controls are implemented and managed by Microsoft. This control is inherited from Microsoft Azure. |

### 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-8 | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter AC-8(a): *<Customer-defined system use notification message or banner>* | |
| Parameter AC-8(c)-1: *<Customer-defined conditions>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-8 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for implementing a compliant system use notification for all customer-deployed resources. The customer control implementation statement should address the content of the notification and the conditions under which it will be displayed.  FedRAMP Requirement: The customer is responsible for determining which customer-deployed resources require a system use notification. The customer control implementation statement should address the resources that require a system notification. The customer is required to obtain JAB/AO approval of said resources. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for requiring users to acknowledge the system use notification (described in AC-08.a) on customer-deployed resources. The customer control implementation statement should address the means by which the user will indicate acknowledgment before continuing.  FedRAMP Requirement: The customer is responsible for providing a mechanism that can periodically verify the system use notification is in place on customer-deployed resources. The customer control implementation statement should address the frequency and process by which the system use notification is verified. The customer is required to obtain JAB/AO approval of the system use notification verification process. |
| Part c | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for displaying a system use notification on all publicly accessible customer-deployed resources. The customer control implementation statement should address the conditions under which the notification will be displayed. The notification will include (if any) descriptions of monitoring, recording, or auditing that may be configured, and the description of authorized uses of the system.  FedRAMP Requirement: The customer is responsible for verifying that the system use notification is being displayed as required on customer-deployed resources, either through a configuration baseline check or via other means. The customer control implementation statement should address the verification process of the system use notification. The customer is required to obtain JAB/AO approval of the verification process. |

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-8 Req. | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-8 What is the solution and how is it implemented? | |
| --- | --- |
| Req. 1 | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for implementing a compliant system use notification for all customer-deployed resources. The customer control implementation statement should address the content of the notification and the conditions under which it will be displayed.  FedRAMP Requirement: The customer is responsible for determining which customer-deployed resources require a system use notification. The customer control implementation statement should address the resources that require a system notification. The customer is required to obtain JAB/AO approval of said resources. |
| Req. 2 | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for requiring users to acknowledge the system use notification (described in AC-08.a) on customer-deployed resources. The customer control implementation statement should address the means by which the user will indicate acknowledgment before continuing.  FedRAMP Requirement: The customer is responsible for providing a mechanism that can periodically verify the system use notification is in place on customer-deployed resources. The customer control implementation statement should address the frequency and process by which the system use notification is verified. The customer is required to obtain JAB/AO approval of the system use notification verification process. |
| Req. 3 | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for displaying a system use notification on all publicly accessible customer-deployed resources. The customer control implementation statement should address the conditions under which the notification will be displayed. The notification will include (if any) descriptions of monitoring, recording, or auditing that may be configured, and the description of authorized uses of the system.  FedRAMP Requirement: The customer is responsible for verifying that the system use notification is being displayed as required on customer-deployed resources, either through a configuration baseline check or via other means. The customer control implementation statement should address the verification process of the system use notification. The customer is required to obtain JAB/AO approval of the verification process. |

### 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: *<Customer-defined>* | |
| Parameter AC-10-1: *<Customer-defined account and/or account type>* | |
| Parameter AC-10-2: *<FedRAMP Assignment: three (3) sessions for privileged access and two (2) sessions for non-privileged access>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-10 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for defining and enforcing the limit of concurrent sessions for each customer-controlled account and/or account type. The customer control implementation statement should address the number of concurrent sessions allowed for each account type. |

### 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-defined>* | |
| Parameter AC-11(a): *<FedRAMP Assignment: fifteen (15) minutes>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-11 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for incorporating a session lock on all customer-deployed resources. The customer control implementation statement should address the period of inactivity and/or user actions resulting in a session lock. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for retaining the session lock until the user reauthenticates on customer-deployed resources. The customer control implementations statement should address the mechanisms used to reauthenticate a user for a locked session. |

#### 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-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-11 (1) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for concealing previously visible information when a session lock is initiated on customer-deployed resources. The customer control implementation statement should address the means by which the displayed information is concealed. |

### 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: *<Customer-defined>* | |
| Parameter AC-12: *<Customer-defined conditions or trigger events requiring session disconnect>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-12 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for defining and enforcing events or conditions requiring the termination of a user session on customer-deployed resources. The customer control implementation statement should address the triggering events or conditions in which the system terminates a user session. |

#### AC-12 (1) Control Enhancement (H)

The information system:

1. Provides a logout capability for user-initiated communications sessions whenever authentication is used to gain access to [Assignment: organization-defined information resources]; and
2. Displays an explicit logout message to users indicating the reliable termination of authenticated communications sessions.

AC-8 Additional FedRAMP Requirements and Guidance:

Guidance: Testing for logout functionality (OTG-SESS-006) https://www.owasp.org/index.php/Testing\_for\_logout\_functionality\_%28OTG-SESS-006%29

| AC-12 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter AC-12(1)(a): *<Customer-defined information resources>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-12 (1) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for providing the capability to logout for all user authenticated sessions on customer-deployed resources. The customer control implementation statement should address the mechanisms in place to provide logout capabilities for user authenticated sessions. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for displaying an explicit logout message to users on customer-deployed resources. The customer control implementation statement should address the content displayed in the logout message. |

### 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: *<Customer-defined>* | |
| Parameter AC-14(a): *<Customer-defined 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-14 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for identifying actions that can be performed on the customer-deployed resources without identification or authentication (e.g., such as viewing a publicly accessible web page). The customer control implementation statement should address the process by which the organization identifies the specific actions that can be performed on the customer system without user identification of authentication. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for providing documentation for user actions not requiring identification or authentication on customer-deployed resources. The customer control implementation statement should address the rationale behind each specific instance of user interaction that does not require identification or authentication. |

### 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-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-17 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for documenting remote access requirements to customer-deployed resources. The customer control implementation statement should address usage restrictions, configuration and connection requirements, and implementation guidance for all remote access types. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for ensuring all remote access connections to customer-deployed resources are authorized. The customer control implementation statement should address the authorizations established in AC-02.i. |

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

The information system monitors and controls remote access methods.

| AC-17 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-17 (1) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for monitoring and controlling remote access methods for customer-deployed resources. The customer control implementation statement should address the techniques used to monitor remote connections. |

#### 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: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-17 (2) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for implementing cryptographic mechanisms (e.g., TLS) to protect remote access sessions to customer-deployed resources. The customer control implementation statement should address cryptographic mechanisms used for remote access sessions. |

#### 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: *<Customer-defined>* | |
| Parameter AC-17(3): *<Customer-defined number>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-17 (3) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for routing remote access connections to customer-deployed resources through managed network access control points. The customer control implementation statement should address the number of access control points used to route remote access. |

#### 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: *<Customer-defined>* | |
| Parameter AC-17(4)(a): *<Customer-defined needs>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-17 (4) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for authorizing privileged commands and access to security-relevant information via remote access for customer-deployed resources. The customer control implementation statement should address the conditions under which privileged commands and access to security-relevant information via remote access may be authorized. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for documenting the rationale for executing privileged commands via remote access for customer-deployed resources. The customer control implementation statement should address privileged commands and their operational need, and document the rationale for the execution of privileged commands via remote access in the system security plan (SSP). |

#### 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: *<Customer-defined>* | |
| Parameter AC-17(9): *<FedRAMP Assignment: fifteen (15) minutes>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-17 (9) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for ensuring the customer-deployed system has the capability to rapidly disconnect or disable remote access. The customer control implementation statement should address the mechanisms used to disconnect remote access sessions and/or disable remote access, and the timeframe within which it must occur. |

### 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: Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-18 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  Microsoft 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 Microsoft Azure environment.  **Customer Responsibility (IaaS/PaaS)**  Microsoft Azure does not permit wireless access within the Azure environment; all wireless protection controls are implemented and managed by Microsoft. This control is inherited from Microsoft Azure. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure does not allow wireless access within Microsoft Azure datacenters.  **Customer Responsibility (IaaS/PaaS)**  Microsoft Azure does not permit wireless access within the Azure environment; all wireless protection controls are implemented and managed by Microsoft. This control is inherited from Microsoft Azure. |

#### 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: Microsoft Azure | |
| Parameter AC-18 (1): 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-18 (1) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure does not allow wireless access within Microsoft Azure datacenters.  **Customer Responsibility (IaaS/PaaS)**  Microsoft Azure does not permit wireless access within the Azure environment; all wireless protection controls are implemented and managed by Microsoft. This control is inherited from Microsoft Azure. |

#### AC-18 (3) Control Enhancement (H)

The organization disables, when not intended for use, wireless networking capabilities internally embedded within information system components prior to issuance and deployment.

| AC-18 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-18 (3) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure does not allow wireless access within Microsoft Azure datacenters.  **Customer Responsibility (IaaS/PaaS)**  Microsoft Azure does not permit wireless access within the Azure environment; all wireless protection controls are implemented and managed by Microsoft. This control is inherited from Microsoft Azure. |

#### AC-18 (4) Control Enhancement (H)

The organization identifies and explicitly authorizes users allowed to independently configure wireless networking capabilities.

| AC-18 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-18 (4) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure does not allow wireless access within Microsoft Azure datacenters.  **Customer Responsibility (IaaS/PaaS)**  Microsoft Azure does not permit wireless access within the Azure environment; all wireless protection controls are implemented and managed by Microsoft. This control is inherited from Microsoft Azure. |

#### AC-18 (5) Control Enhancement (H)

The organization selects radio antennas and calibrates transmission power levels to reduce the probability that usable signals can be received outside of organization-controlled boundaries.

| AC-18 (5) | Control Summary Information |
| --- | --- |
| Responsible Role: Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-18 (5) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure does not allow wireless access within Microsoft Azure datacenters.  **Customer Responsibility (IaaS/PaaS)**  Microsoft Azure does not permit wireless access within the Azure environment; all wireless protection controls are implemented and managed by Microsoft. This control is inherited from Microsoft Azure. |

### 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: Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-19 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure does not allow mobile devices within the Azure boundary. As such, this control is not applicable to Microsoft Azure.  **Customer Responsibility (IaaS/PaaS)**  There are no customer-controlled mobile devices within the scope of systems deployed on Azure; all mobile device protection controls are implemented and managed by Microsoft. This control is inherited from Azure. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure does not allow mobile devices within the Azure boundary. As such, this control is not applicable to Microsoft Azure.  **Customer Responsibility (IaaS/PaaS)**  There are no customer-controlled mobile devices within the scope of systems deployed on Azure; all mobile device protection controls are implemented and managed by Microsoft. This control is inherited from Azure. |

#### 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: Microsoft Azure | |
| Parameter AC-19(5)-1: Not Applicable | |
| Parameter AC-19(5)-2: 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-19 (5) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure does not allow mobile devices within the Azure boundary. As such, this control is not applicable to Microsoft Azure.  **Customer Responsibility (IaaS/PaaS)**  Microsoft Azure does not permit wireless access within the Azure environment; all wireless protection controls are implemented and managed by Microsoft. This control is inherited from Microsoft Azure. |

### 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-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-20 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for establishing terms and conditions allowing authorized individuals to access the customer-deployed resources from external information systems. The customer control implementation statement should address the terms and conditions for access and the external information systems to which those terms and conditions apply. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for establishing terms and conditions allowing authorized individuals to process, store, or transmit customer-controlled information using external information systems. The customer control implementation statement should address the terms and conditions for use of customer-controlled information and the external information systems to which those terms and conditions apply. |

#### 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-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-20 (1) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for establishing terms and conditions for external systems accessing, processing, storing or transmitting organization-defined information from customer-deployed resources. The customer control implementation statement should address the external organization, the corresponding connection or processing agreement, and how the external systems connecting to customer-deployed resources are verified as adhering to the required security controls. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for establishing terms and conditions for external systems accessing, processing, storing or transmitting organization-defined information from customer-deployed resources. The customer control implementation statement should address the external organization, the corresponding connection or processing agreement, and how the external systems connecting to customer-deployed resources are verified as adhering to the required security controls. |

#### 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: Microsoft Azure | |
| Parameter AC-20(2): 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-20 (2) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft does not allow customer-controlled portable storage devices within the Microsoft Azure environment.  **Customer Responsibility (IaaS/PaaS)**  Customers do not have physical access to any system resources in Microsoft Azure datacenters and there are no customer-controlled portable storage devices within the scope of systems deployed on Microsoft Azure. As such, this control is inherited from Microsoft Azure. |

### 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-defined>* | |
| Parameter AC-21(a): *<Customer-defined information sharing circumstances where user discretion is required>* | |
| Parameter AC-21(b): *<Customer-defined automated mechanisms or 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-21 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for determining when authorized users are required to use discretion as to whether to share customer-controlled information. The customer control implementation statement should address the circumstances where user discretion is required. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for employing a process to assist users with making information sharing decisions (see AC-21.a). The customer control implementation statement should address the process used to assist customers with these 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: *<Customer-defined>* | |
| Parameter AC-22: *<FedRAMP Assignment: at least quarterly>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-22 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for designating authorized personnel to post publicly accessible information on customer-deployed resources. The customer control implementation statement should address the personnel authorized to post publicly available content. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for training the personnel defined in AC-21.a to prevent disclosure of nonpublic customer-controlled information. The customer control implementation statement should address the training provided. |
| Part c | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for reviewing proposed content of customer-controlled information prior to posting publicly to ensure nonpublic information is not included. The customer control implementation statement should address the review process. |
| Part d | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for periodically reviewing publicly available customer-controlled content for nonpublic information. The customer control implementation statement should address the frequency of the review and the removal of nonpublic information, if discovered. |

## Awareness and Training (AT)

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

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 annually]; and
   2. Security awareness and training procedures [FedRAMP Assignment: at least annually or whenever a significant change occurs].

| AT-1 | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter AT-1(a): *<Customer-defined personnel or roles>* | |
| Parameter AT-1(b)(1): *<FedRAMP Assignment: at least annually>* | |
| Parameter AT-1(b)(2): *<FedRAMP Assignment: at least annually or whenever a significant change occurs>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| AT-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for developing, documenting, reviewing, updating, and disseminating security awareness training policy and procedures. The customer security awareness training addresses the security around the customer-deployed resources for the customer’s users. The customer control implementation statement should address the content of the policy (which must include purpose, scope, roles, responsibilities, management commitment, coordination, and compliance), procedures (which must facilitate the implementation of the policies and associated controls), the frequency of review, and the role(s) responsible. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for developing, documenting, reviewing, updating, and disseminating security awareness training policy and procedures. The customer security awareness training addresses the security around the customer-deployed resources for the customer’s users. The customer control implementation statement should address the content of the policy (which must include purpose, scope, roles, responsibilities, management commitment, coordination, and compliance), procedures (which must facilitate the implementation of the policies and associated controls), the frequency of review, and the role(s) responsible. |

### 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-defined>* | |
| Parameter AT-2(c): <FedRAMP Assignment: 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AT-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for providing basic security awareness training to all users of customer-deployed resources as part of initial training. The customer control implementation statement should address the content of the training and the process for ensuring all users undergo the initial described training. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for providing updated basic security awareness training to all users when required by changes to customer-deployed resources. The customer control implementation statement should address the system changes that require updated training and the process which ensures all employees receive retraining. |
| Part c | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for providing ongoing, periodic basic security awareness training to all users. The customer control implementation statement should address the frequency at which retraining will occur and the process which ensures all employees receive retraining. |

#### AT-2 (2) Control Enhancement (M) (H)

The organization includes security awareness training on recognizing and reporting potential indicators of insider threat.

| AT-2 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AT-2 (2) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for providing training on insider threats. The customer control implementation statement should address the indicators of insider threats, and the process of recognizing and reporting them. |

### 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-defined>* | |
| Parameter AT-3(c): <FedRAMP Assignment: 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AT-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for providing role-based security training to users before authorizing access to customer-deployed resources or performing assigned duties. The customer control implementation statement should address the content of the training for each identified role, and the process for ensuring all identified roles receive training prior to accessing the system or performing assigned duties. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for providing role-based security training to all identified roles when required by changes to customer-deployed resources. The customer control implementation statement should address the system changes that require updated training and the process which ensures all employees receive retraining. |
| Part c | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for providing ongoing, periodic role-based security training to all identified roles. The customer control implementation statement should address the frequency at which retraining will occur and the process which ensures all employees receive retraining. |

#### AT-3 (3) Control Enhancement (H)

The organization includes practical exercises in security training that reinforce training objectives.

| AT-3 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AT-3 (3) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for providing role-based practical exercises to reinforce training objectives established in AT-03. The customer control implementation statement should address the training exercises included for identified roles. |

#### AT-3 (4) Control Enhancement (H)

The organization provides training to its personnel on [FedRAMP Assignment: malicious code indicators as defined by organization incident policy/capability] to recognize suspicious communications and anomalous behavior in organizational information systems.

| AT-3 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter AT-3 (4): *<FedRAMP Assignment: malicious code indicators as defined by organization incident policy/capability>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AT-3 (4) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for providing role-based training on suspicious communications and anomalous behavior within customer-deployed resources. The customer control implementation statement should address the indicators of malicious code and the process for recognizing suspicious communications and anomalous behavior. |

### AT-4 Security Training Records (H)

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 five (5) years or 5 years after completion of a specific training program].

| AT-4 | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter AT-4(b): <FedRAMP Assignment: at least five (5) years or 5 years after completion of a specific training program> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AT-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for documenting and monitoring all system security training activities for customer-deployed resources. The customer control implementation statement should address the process used to monitor and document training. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for retaining individual training records for users of customer-deployed resources. The customer control implementation statement should address the retention period for individual training records. |

## Audit and Accountability (AU)

### AU-1 Audit and Accountability Policy and Procedures (H)

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 least annually]; and
   2. Audit and accountability procedures [FedRAMP Assignment: at least annually or whenever a significant change occurs].

| AU-1 | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter AU-1(a): <*FedRAMP Assignment: organization-defined personnel or roles*> | |
| Parameter AU-1(b)(1): <*FedRAMP Assignment: at least annually*> | |
| Parameter AU-1(b)(2): <*FedRAMP Assignment: at least annually or whenever a significant change occurs*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| AU-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for developing, documenting, reviewing, updating, and disseminating audit and accountability policy and procedures. These documents should address the auditing and accountability of the customer-deployed system. The customer control implementation statement should address the content of the policy (which must include purpose, scope, roles, responsibilities, management commitment, coordination, and compliance), procedures (which must facilitate the implementation of the policies and associated controls), the frequency of review, and the role(s) responsible. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for developing, documenting, reviewing, updating, and disseminating audit and accountability policy and procedures. These documents should address the auditing and accountability of the customer-deployed system. The customer control implementation statement should address the content of the policy (which must include purpose, scope, roles, responsibilities, management commitment, coordination, and compliance), procedures (which must facilitate the implementation of the policies and associated controls), the frequency of review, and the role(s) responsible. |

### 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-2 | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer-defined*>*;* Microsoft Azure | |
| Parameter AU-2(a): <*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*> | |
| Parameter AU-2(d): <*FedRAMP Assignment: organization-defined subset of the auditable events defined in AU-2 a. to be audited continually for each identified event*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AU-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (PaaS)**  Microsoft Azure implements auditing at the VM level on behalf of PaaS customers.  Microsoft Azure has developed a general set of auditable events applicable to Microsoft Azure VMs based on ongoing risk assessments of the system. The audit policy is set as part of the baseline image deployed when the VM is created. Microsoft Azure reviews the general event set when a significant change to the system is made to ensure that any vulnerabilities exposed are being addressed by the set of auditable events.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (PaaS)**  The customer is responsible for ensuring the system is capable of auditing customer-defined events for customer-deployed resources (to include applications, databases, and software). The customer control implementation statement should address the identified events and the system's capability to audit them.  **Customer Responsibility (IaaS)**  The customer is responsible for ensuring the system is capable of auditing customer-defined events for customer-deployed resources (to include applications, operating systems, databases, and software). The customer control implementation statement should address the identified events and the system's capability to audit them. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for coordinating with other entities within its organization to guide the selection of auditable events for customer-deployed resources. The customer control implementation statement should address the customer's organizational entities that provide input to the selection of auditable events and the process by which auditable event selection is coordinated. |
| Part c | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for ensuring the list of auditable events supports after-the-fact investigations of customer-deployed resources. The customer control implementation statement should address the rationale for why the auditable events defined in AU-02.a are adequate to support after-the-fact investigations. |
| Part d | **Microsoft Azure (PaaS)**  Microsoft Azure implements auditing at the VM level on behalf of PaaS customers.  The audit policy for the OS image defines the events that must be audited. Events are audited continually.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for selecting a subset of the events defined in AU-02.a to be audited on customer-deployed resources. The customer control statement should address the subset of auditable events, and the frequency of (and/or situations requiring) auditing for each identified event. |

#### 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-2 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer-defined*>;Microsoft Azure | |
| Parameter AU-2(3): <*FedRAMP Assignment: 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AU-2 (3) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (PaaS)**  Microsoft Azure’s Security and OSSC SIM teams maintain and review a list of auditable events at least annually and make updates in the Azure Security Pack. Application-specific events are reviewed annually by these teams 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 Microsoft Azure by the JAB.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for reviewing and updating the events defined in AU-02. The customer control implementation statement should address the process and frequency of reviewing and updating the auditable events defined in AU-02. |

### 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-3 | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer-defined*>*;* Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AU-3 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (PaaS)**  Microsoft Azure implements auditing requirements at the VM level on behalf of PaaS customers.  Per the Microsoft Azure Logging and Monitoring SOP (which is available for 3PAO review onsite), 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 * Type * Outcome (success/failure) * Bytes sent/received – as relevant/appropriate for event type * 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. Microsoft Azure does not filter any of the content generated.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for configuring Azure auditing capabilities on customer-deployed (to include applications, databases, and software) resources to generate audit records. The customer control implementation statement should address the requirement that audit records contain the following: what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event and the identity of any subjects associated with the event.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for configuring Azure auditing capabilities on customer-deployed (to include applications, operating systems, databases, and software) resources to generate audit records. The customer control implementation statement should address the requirement that audit records contain the following: what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event and the identity of any subjects associated with the event. |

#### AU-3 (1) Control Enhancement (H)

The information system generates audit records containing the following additional information: [FedRAMP 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; individual identities of group account users; full-text of privileged commands]. The audit record types are approved and accepted by the JAB/AO.

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

| AU-3 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer-defined*>;Microsoft Azure | |
| Parameter AU-3(1): <*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; individual identities of group account users; full-text of privileged commands> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AU-3 (1) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (PaaS)**  Microsoft Azure implements auditing requirements at the VM level on behalf of PaaS customers.  Microsoft Azure collects the audit record content specified in AU-3, which includes the additional information specified in this control. This content includes informational messages to diagnose or identify events, characteristics that describe or identify the object or resource being acted upon, and the number of bytes received and bytes sent, all of which will vary by event type. The session, connection, transaction, or activity duration can be obtained by analyzing the audit records collected; events related to sessions, connections and transactions will contain timestamps which can be analyzed to determine duration.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for configuring Azure auditing capabilities on customer-deployed resources to ensure organizational audit record content requirements are implemented. The customer control implementation statement should address customer-defined details required in audit records in addition to the contents specified in AU-03. |

#### AU-3 (2) Control Enhancement (H)

The information system provides centralized management and configuration of the content to be captured in audit records generated by [FedRAMP Assignment: all network, data storage, and computing devices].

| AU-3 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>;* Microsoft Azure | |
| Parameter AU-3 (2): *<FedRAMP Assignment: all network, data storage, and computing devices>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AU-3 (2) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (PaaS)**  Microsoft Azure implements auditing requirements at the VM level on behalf of PaaS customers.  Microsoft Azure Security provides centralized management and configuration of audit record generation through the Azure Monitoring and Diagnostics Service, which is used for virtual machines. Teams using physical servers have deployed Windows Event Collector (WEC) as part of their standard configuration.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (PaaS)**  The customer is responsible for implementing centralized management and configuration of the content to be captured in audit records of customer-deployed resources (to include applications, databases, and software). The customer control implementation statement should address the centralized management and configuration tool(s), and the system components which generate audit records.  **Customer Responsibility (IaaS)**  The customer is responsible for implementing centralized management and configuration of the content to be captured in audit records of customer-deployed resources (to include applications, operating systems, databases, and software). The customer control implementation statement should address the centralized management and configuration tool(s), and the system components which generate audit records. |

### 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-4 | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer-defined*>;Microsoft Azure | |
| Parameter AU-4: <*Customer-defined audit record storage 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AU-4 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (PaaS)**  Microsoft Azure implements auditing requirements at the VM level on behalf of PaaS customers.  The Storage team contacts the component team whenever a pre-determined threshold for auditing failures or capacity is crossed. Storage capacity can be increased in the following manner:  Audit records for each of the Microsoft Azure services are captured by the Monitoring Agent (MA) and retained in xStore. Each xStore storage account is allocated sufficient storage capacity for the retention of at least 90 days’ worth of logs and is monitored for usage by the service component teams. If an account is near capacity, service teams are notified by the Storage team and the appropriate component teams will create an additional storage account to expand the capacity.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (PaaS)**  The customer is responsible for allocating audit record storage capacity for customer-deployed resources (to include applications, databases, and software). The customer control implementation statement should address the audit record storage requirements. Additionally, the customer should consider the retention period defined in AU-11 when allocating storage capacity for audit records.  **Customer Responsibility (IaaS)**  The customer is responsible for allocating audit record storage capacity for customer-deployed resources (to include applications, operating systems, databases, and software). The customer control implementation statement should address the audit record storage requirements. Additionally, the customer should consider the retention period defined in AU-11 when allocating storage capacity for audit records. |

### 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-5 | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer-defined*>;Microsoft Azure | |
| Parameter AU-5(a): <*FedRAMP Assignment: organization-defined personnel or roles*> | |
| Parameter AU-5(b): <*FedRAMP Assignment: organization-defined actions to be taken; (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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AU-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (PaaS)**  Microsoft Azure implements auditing requirements at the VM level on behalf of PaaS customers.  Potential events and incidents are notified to the component teams or Microsoft Azure Live Site (WALS) team through multiple channels, including Azure Security Monitoring (ASM), Alert and Incident Management System (AIMS), System Center Operations Manager (SCOM), customers, and vendors.  ASM is responsible for capturing security log events and storing them in Monitoring and Diagnostic Service (MDS) tables. AIMS is an automated mechanism for scanning tables and raising alerts when specific predefined criteria is met; AIMS generates email notifications and creates a corresponding Incident Management (IcM) ticket. AIMS actively monitors the production environment based on the filters and the thresholds identified within the rules defined by the Azure Security team and respective component teams.  Azure-based (virtual machines and web/worker role instances) services have AIMS alerts defined for monitoring audit infrastructure health and security and generating alerts. OrgID uses SCOM for monitoring audit infrastructure and security and generating alerts. All alerts follow the procedures outlined in the Incident Response controls, which include analysis to determine whether further action is necessary.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (PaaS)**  The customer is responsible for providing alerts in response to audit processing failures (e.g., storage quota is reached, audit hardware/software errors) of customer-deployed resources (to include applications, databases, and software). The customer control implementation statement should address the personnel/roles to be notified when audit processing failures occur.  **Customer Responsibility (IaaS)**  The customer is responsible for providing alerts in response to audit processing failures (e.g., storage quota is reached, audit hardware/software errors) of customer-deployed resources (to include applications, operating systems, databases, and software). The customer control implementation statement should address the personnel/roles to be notified when audit processing failures occur. |
| Part b | **Microsoft Azure (PaaS)**  Microsoft Azure implements auditing requirements at the VM level on behalf of PaaS customers.  FedRAMP parameter requirements state that in the case of audit processing failures, a moderate-impact system must shut down. It is impractical for Microsoft Azure to take this action from a business standpoint. While a failure in audit processing would create the risk of being unable to perform comprehensive after-the-fact investigation of a security incident, this risk is not sufficient to justify the disruption of service and loss of business that would result from shutting down the system.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for taking action when audit processing failures occur for customer-deployed resources. The customer control implementation statement should address what actions are to be taken in the event of an audit processing failure. |

#### AU-5 (1) Control Enhancement (H)

The information system provides a warning to [Assignment: organization-defined personnel, roles, and/or locations] within [Assignment: organization-defined time period] when allocated audit record storage volume reaches [Assignment: organization-defined percentage] of repository maximum audit record storage capacity.

| AU-5 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>;* Microsoft Azure | |
| Parameter AU-5 (1)-1: *<FedRAMP Assignment: organization-defined personnel, roles, and/or locations>* | |
| Parameter AU-5 (1)-2: *<FedRAMP Assignment: organization-defined time period>* | |
| Parameter AU-5 (1)-3: *<FedRAMP Assignment: organization-defined percentage>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AU-5 (1) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (PaaS)**  Microsoft Azure implements auditing requirements at the VM level on behalf of PaaS customers.  Automated messages are sent out alerting component teams whenever a pre-determined threshold for auditing failures or capacity is crossed. Storage capacity can be increased in the following manner:  Audit records for each of the Microsoft Azure Government services are captured by the Monitoring Agent (MA) and retained in xStore. Each xStore storage account is allocated sufficient storage capacity for the retention of at least 90 days’ worth of logs and is monitored for usage by the service component teams. If an account is near capacity, a pre-defined alert will generate a ticket and the appropriate component team will create an additional storage account to expand the capacity.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (PaaS)**  The customer is responsible for configuring an audit record storage capacity warning for customer-deployed resources (to include applications, databases, and software). The customer control implementation statement should address the percentage of storage capacity at which a warning is required; the time period within which the warning must occur; and the personnel, roles, and/or locations to be notified.  **Customer Responsibility (IaaS)**  The customer is responsible for configuring an audit record storage capacity warning for customer-deployed resources (to include applications, operating systems, databases, and software). The customer control implementation statement should address the percentage of storage capacity at which a warning is required; the time period within which the warning must occur; and the personnel, roles, and/or locations to be notified. |

#### AU-5 (2) Control Enhancement (H)

The information system provides an alert in [FedRAMP Assignment: organization-defined real-time] to [FedRAMP Assignment: service provider personnel with authority to address failed audit events] when the following audit failure events occur: [FedRAMP Assignment: audit failure events requiring real-time alerts, as defined by organization audit policy].

| AU-5 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>;* Microsoft Azure | |
| Parameter AU-5 (1)-1: *<FedRAMP Assignment: organization-defined real-time>* | |
| Parameter AU-5 (1)-2: *<FedRAMP Assignment: service provider personnel with authority to address failed audit events>* | |
| Parameter AU-5 (1)-3: *<FedRAMP Assignment: audit failure events requiring real-time alerts, as defined by organization audit 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AU-5 (2) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (PaaS)**  Microsoft Azure implements auditing requirements at the VM level on behalf of PaaS customers.  Azure-based services have alerts defined for monitoring audit infrastructure health and security and generating alerts. Those mechanisms generate real-time alerts when audit failures occur.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (PaaS)**  The customer is responsible for providing real-time alerts for audit event failures for customer-deployed resources (to include applications, databases, and software). The customer control implementation statement should address the audit failure events requiring real-time alerts, the time period within which alerts must occur; and the personnel, roles, and/or locations to be notified.  **Customer Responsibility (IaaS)**  The customer is responsible for providing real-time alerts for audit event failures for customer-deployed resources (to include applications, operating systems, databases, and software). The customer control implementation statement should address the audit failure events requiring real-time alerts, the time period within which alerts must occur; and the personnel, roles, and/or locations to be notified. |

### 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-6 | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer-defined*>*;* Microsoft Azure | |
| Parameter AU-6(a)-1: <*FedRAMP Assignment: at least weekly*> | |
| Parameter AU-6(a)-2: <*FedRAMP Assignment: organization-defined inappropriate or unusual activity*> | |
| Parameter AU-6(b): <*FedRAMP Assignment: organization-defined personnel or roles*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AU-6 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (PaaS)**  Microsoft Azure implements auditing requirements at the VM level on behalf of PaaS customers.  Audit log review occurs at least weekly and in the case of a security incident, customer request or escalation, or any other functionality impacting the incident in production. Audit records are reviewed and analyzed for indications of inappropriate or unusual activity, including the indications of compromise identified in SI-4(5).  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (PaaS)**  The customer is responsible for reviewing and analyzing audit records of customer-deployed resources (to include applications, databases, and software). The customer control implementation statement should address the frequency at which the audit records are reviewed and analyzed, and the criteria used to identify inappropriate or unusual activity.  **Customer Responsibility (IaaS)**  The customer is responsible for reviewing and analyzing audit records of customer-deployed resources (to include applications, operating systems, databases, and software). The customer control implementation statement should address the frequency at which the audit records are reviewed and analyzed, and the criteria used to identify inappropriate or unusual activity. |
| Part b | **Microsoft Azure (PaaS)**  Microsoft Azure implements auditing requirements at the VM level on behalf of PaaS customers.  Audit review findings are reported and escalated using standard security incident management channels. Depending on the type of issue, TFS or Incident Management (ICM) tickets are opened to track resolution of the incident.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for reporting findings of inappropriate or unusual activity (defined in AU-06.a) on customer-deployed resources. The customer control implementation statement should address which personnel/roles will be notified of any findings. |

#### 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-6 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>;* Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AU-6 (1) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (PaaS)**  Microsoft Azure implements auditing requirements at the VM level on behalf of PaaS customers.  Service Application Layer  The audit tools deployed in Azure-based services (as described in AU-5) provide the capability to generate customizable reporting capabilities based on selectable event criteria. As necessary, Microsoft Azure administrators increase the level of auditing and analyze activity in response to higher risks. MDS provides the capability for audit review, analysis, and reporting to support the incident response procedures as defined in the Microsoft Azure IR controls.  Additionally, ASM runs as MDS Runner and aggregates analysis such as anomaly detection (clustering), filtering and whitelisting rules, etc. ASM can generate Summary Reports using predefined queries.  OS Layer  The Microsoft Azure Security team captures OS Events of interest to report and alert on suspicious activities. The reports are generated using Cosmos scope jobs. ASM analyzes OS event distribution to identify spikes in event traffic, MDS and deployment.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (PaaS)**  The customer is responsible for automating the audit review, analysis, and reporting of suspicious activities within customer-deployed resources (to include applications, databases, and software). The customer control implementation statement should address the automated mechanisms employed to support investigation and response to suspicious activities.  **Customer Responsibility (IaaS)**  The customer is responsible for automating the audit review, analysis, and reporting of suspicious activities within customer-deployed resources (to include applications, operating systems, databases, and software). The customer control implementation statement should address the automated mechanisms employed to support investigation and response to suspicious activities. |

#### AU-6 (3) Control Enhancement (M) (H)

The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.

| AU-6 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer-defined*>*;* Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AU-6 (3) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (PaaS)**  Microsoft Azure implements auditing requirements at the VM level on behalf of PaaS customers.  The Microsoft Azure Security team correlates log files across multiple Microsoft Azure systems team using a combination of tools.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for analyzing and correlating audit records (defined in AU-06) across customer-deployed repositories. The customer control implementation statement should address the repositories used and how audit records are correlated across them to gain organization-wide situational awareness. |

#### AU-6 (4) Control Enhancement (H)

The information system provides the capability to centrally review and analyze audit records from multiple components within the system.

| AU-6 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>;* Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AU-6 (4) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (PaaS)**  Microsoft Azure implements auditing requirements at the VM level on behalf of PaaS customers.  Microsoft Azure Security performs centralized review and analysis of audit records across all components of Microsoft Azure.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (PaaS)**  The customer is responsible for providing the capability to centrally review and analyze audit records collected from customer-deployed resources (to include applications, databases, and software). The customer control implementation statement should address the central review and analysis process and the resources generating the audit records.  **Customer Responsibility (IaaS)**  The customer is responsible for providing the capability to centrally review and analyze audit records collected from customer-deployed resources (to include applications, operating systems, databases, and software). The customer control implementation statement should address the central review and analysis process and the resources generating the audit records. |

#### AU-6 (5) Control Enhancement (H)

The organization integrates analysis of audit records with analysis of [FedRAMP Selection (one or more): vulnerability scanning information; performance data; information system monitoring information; penetration test data; [Assignment: organization-defined data/information collected from other sources]] to further enhance the ability to identify inappropriate or unusual activity.

| AU-6 (5) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter AU-6 (5): *<FedRAMP Assignment: organization-defined data/information collected from other sources>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AU-6 (5) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for integrating audit record analysis with analysis of data/information collected from other sources to further identify suspicious activity within customer-deployed resources. The customer control implementation statement should address the additional data/information collected (i.e., vulnerability scan data, performance data, system monitoring data, and/or other customer-defined data). |

#### AU-6 (6) Control Enhancement (H)

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

AU-6 Additional FedRAMP Requirements and Guidance:

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

| AU-6 (6) | Control Summary Information |
| --- | --- |
| Responsible Role: Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AU-6 (6) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure’s SIM team uses the related physical monitoring data and correlates it with audit records to determine if there was any associated logical breach or suspicious behavior when physical incidents are detected.  **Customer Responsibility (IaaS/PaaS)**  Customers do not have access to any physical system components in Azure datacenters; all physical resources are audited and managed by Microsoft Azure. This control is inherited from Azure. |

#### AU-6 (7) Control Enhancement (H)

The organization specifies the permitted actions for each [FedRAMP Selection (one or more): information system process; role; user] associated with the review, analysis, and reporting of audit information.

| AU-6 (7) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>,* Microsoft Azure | |
| Parameter AU-6 (7): *<FedRAMP Selection (one or more): information system process; role; user>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AU-6 (7) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (PaaS)**  Microsoft Azure implements auditing requirements at the VM level on behalf of PaaS customers.  Microsoft Azure Government specifies the permitted actions for each process, role, or user via Role-Based Access Control. Security groups are defined in the Microsoft tools; each security group has specified access rights and permitted actions.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for specifying the permitted actions associated with the review, analysis, and reporting of customer-controlled audit information. The customer control implementation statement should address the permitted actions for each identified process, role, and/or user. |

#### AU-6 (10) Control Enhancement (H)

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

| AU-6 (10) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>;* Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AU-6 (10) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (PaaS)**  Microsoft Azure implements auditing requirements at the VM level on behalf of PaaS customers.  Microsoft Azure Security receives alerts from vendor Web sites, other third-party services (Internet Security Systems, US-CERT advisories and alerts), and Microsoft-published bulletins, and 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.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (PaaS)**  The customer is responsible for adjusting the level of audit review, analysis, and reporting for customer-deployed resources (to include applications, databases, and software) when there is a change in risk based on information provided by law enforcement, intelligence, or other credible sources. The customer control implementation statement should address the ability to scale the audit review process.  **Customer Responsibility (IaaS)**  The customer is responsible for adjusting the level of audit review, analysis, and reporting for customer-deployed resources (to include applications, operating systems, databases, and software) when there is a change in risk based on information provided by law enforcement, intelligence, or other credible sources. The customer control implementation statement should address the ability to scale the audit review process. |

### 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-7 | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer-defined*>*;* Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AU-7 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (PaaS)**  Microsoft Azure implements auditing requirements at the VM level on behalf of PaaS customers.  Microsoft Azure service teams have deployed Azure Monitoring and Diagnostics Service (MDS) as part of a virtual environment-wide monitoring solution. This tool also provides the capability to digest large amounts of log data into human readable reports. Microsoft Azure Security uses this tool to analyze and reduce the audit logs in order to generate actionable reports that the service teams can use for after-the-fact investigations of security incidents, to correct vulnerabilities, and to address any weaknesses found.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (PaaS)**  The customer is responsible for providing an audit reduction and report generation capability for customer-deployed resources (to include applications, databases, and software). The customer control implementation statement should address how the system supports on-demand audit review, analysis, and reporting requirements, and after-the-fact investigations of security incidents.  **Customer Responsibility (IaaS)**  The customer is responsible for providing an audit reduction and report generation capability for customer-deployed resources (to include applications, operating systems, databases, and software). The customer control implementation statement should address how the system supports on-demand audit review, analysis, and reporting requirements, and after-the-fact investigations of security incidents. |
| Part b | **Microsoft Azure (PaaS)**  Microsoft Azure implements auditing requirements at the VM level on behalf of PaaS customers.  The tools used in Microsoft Azure to collect and process audit records do not permanently or irreversibly alter the original audit record content or time ordering.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for ensuring the original content and time ordering of customer-controlled audit records is not altered. The customer control implementation statement should address how the process defined in AU-07.a maintains audit record integrity. |

#### 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-7 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer-defined*>;Microsoft Azure | |
| Parameter AU-7(1): *<FedRAMP Assignment: organization-defined audit 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AU-7 (1) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (PaaS)**  Microsoft Azure implements auditing requirements at the VM level on behalf of PaaS customers.  The incoming stream of events are aggregated, correlated, duplicated, and reduced into security or service relevant alerts and alarms that are used by the services to analyze and respond appropriately to suspicious activity. Authorized personnel are able to query the system and generate reports that are used to review events or investigate specific activities, as required by the Microsoft Azure Security Policy.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for providing the capability to process customer-controlled audit records for events of interest. The customer control implementation statement should address the customer-defined audit fields on which the events of interest will be based. |

### 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-8 | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer-defined*>;Microsoft Azure | |
| Parameter AU-8(b): <*FedRAMP Assignment: one second granularity of time measurement*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AU-8 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (PaaS)**  Microsoft Azure implements auditing requirements at the VM level on behalf of PaaS customers.  For all asset types, all audit records and events generated within Microsoft Azure capture the time stamp from the internal system clock of the component that generated the event.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (PaaS)**  The customer is responsible for generating time stamps for audit records of customer-deployed resources (to include applications, databases, and software). The customer control implementation statement should address how internal system clocks are used to time-stamp audit records.  **Customer Responsibility (IaaS)**  The customer is responsible for generating time stamps for audit records of customer-deployed resources (to include applications, operating systems, databases, and software). The customer control implementation statement should address how internal system clocks are used to time-stamp audit records. |
| Part b | **Microsoft Azure (PaaS)**  Microsoft Azure implements auditing requirements at the VM level on behalf of PaaS customers.  Microsoft Azure records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC). Time stamps are generated either in UTC directly or in local time with an offset from UTC. Microsoft Azure time stamps are precise at least to the millisecond.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for ensuring customer-controlled audit records have time stamps that are recorded and can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT). The customer control implementation statement should define the process for mapping time stamps to UTC or GMT and the granularity of time measurement to be captured (e.g., hundreds of milliseconds or tens of milliseconds). |

#### 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*](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-8 (1) Additional FedRAMP Requirements and Guidance:

Requirement: The service provider selects primary and secondary time servers used by the NIST Internet time service. The secondary server is selected from a different geographic region than the primary server.

Requirement: The service provider synchronizes the system clocks of network computers that run operating systems other than Windows to the Windows Server Domain Controller emulator or to the same time source for that server.

Guidance: 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-8 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer-defined*>*;* Microsoft Azure | |
| Parameter AU-8(1)(a)-1: <*FedRAMP Assignment: authoritative time source*> | |
| Parameter AU-8(1)(a)-2: <*FedRAMP Assignment: at least hourly*> | |
| Parameter AU-8(1)(b): <*FedRAMP Assignment: organization-defined time period*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AU-8 (1) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (PaaS)**  Microsoft Azure implements auditing requirements at the VM level on behalf of PaaS customers.  For virtual services, all services are configured to use the Coordinated Universal Time (UTC) setting when generating event logs in Storage tables.  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 datacenter time servers.  The datacenter time servers are NTP Stratum 1 time servers that sync from the Global Positioning System (GPS) satellites. Microsoft Azure manages two different NTP time servers in separate geographic locations. The time servers are geographically dispersed and located in 2 separate Microsoft-managed datacenters in the CONUS. Microsoft Azure chooses to use the GPS satellites as the authoritative time source as an alternative to the NIST time hosts.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for comparing internal system clocks with an authoritative time source. The customer control implementation statement should address the authoritative time source selected and the frequency of comparison.  FedRAMP Requirement: The customer is responsible for selecting time servers used by the NIST Internet time service. The customer control implementation statement should address the primary NIST time server selected and a secondary NIST time server selected from a different geographic region. |
| Part b | **Microsoft Azure (PaaS)**  Microsoft Azure implements auditing requirements at the VM level on behalf of PaaS customers.  All Microsoft Azure 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.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for synchronizing internal system clocks to the authoritative time source defined in AU-08(01)a. The customer control implementation statement should address the time difference at which synchronization must occur.  FedRAMP Requirement: The customer is responsible for synchronizing non-Windows systems to the organization's authoritative time source. The customer control implementation statement should address which internet time services are used for non-Windows systems. |

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: Synchronization of system clocks improves the accuracy of log analysis.

| AU-8 (1) Req. | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>;* Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AU-8 (1) What is the solution and how is it implemented? | |
| --- | --- |
| Req. 1 | **Microsoft Azure (PaaS)**  Microsoft Azure implements auditing requirements at the VM level on behalf of PaaS customers.  All Microsoft Azure 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.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for synchronizing internal system clocks to the authoritative time source defined in AU-08(01)a. The customer control implementation statement should address the time difference at which synchronization must occur.  FedRAMP Requirement: The customer is responsible for synchronizing non-Windows systems to the organization's authoritative time source. The customer control implementation statement should address which internet time services are used for non-Windows systems. |
| Req. 2 | **Microsoft Azure (PaaS)**  Microsoft Azure implements auditing requirements at the VM level on behalf of PaaS customers.  All Microsoft Azure 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.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for synchronizing internal system clocks to the authoritative time source defined in AU-08(01)a. The customer control implementation statement should address the time difference at which synchronization must occur.  FedRAMP Requirement: The customer is responsible for synchronizing non-Windows systems to the organization's authoritative time source. The customer control implementation statement should address which internet time services are used for non-Windows systems. |

### 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-9 | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer-defined*>;Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AU-9 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (PaaS)**  Microsoft Azure implements protection of audit information through the use of an authenticated and encrypted connection from the node to the centralized audit collection system MDS. Access to the centralized audit collection systems is restricted to the Security Engineering and Operations groups based on the standard access groups defined for Azure.  As a result, only authorized personnel are allowed access to audit records and their assigned rights prohibit them from modifying or deleting audit information.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for preventing unauthorized access to audit information and tools. The customer implementation statement should address the mechanisms preventing unauthorized access modification and deletion. |

#### 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-9 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer-defined*>;Microsoft Azure | |
| Parameter AU-9(2): <*FedRAMP Assignment: 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AU-9 (2) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (PaaS)**  Microsoft Azure implements auditing requirements at the VM level on behalf of PaaS customers.  Audit logs are backed up to Azure Storage accounts in near real time. In the event that real-time log shipping fails, logs are retained on the server until they can be exported to the appropriate central storage location.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for backing up customer-controlled audit records to a physically different system. The customer control implementation statement should address backup frequency and how the backup destination is separated physically from the source. |

#### AU-9 (3) Control Enhancement (H)

The information system implements cryptographic mechanisms to protect the integrity of audit information and audit tools.

| AU-9 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>;* Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AU-9 (3) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (PaaS)**  Microsoft Azure implements auditing requirements at the VM level on behalf of PaaS customers.  Microsoft Azure encrypts all audit log data stored within the Storage Accounts used for audit log retention.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for maintaining the integrity of the customer-controlled audit system. The customer control implementation statement should address the cryptographic mechanisms in place to protect audit information and tools. |

#### 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-9 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer-defined*>;Microsoft Azure | |
| Parameter AU-9(4): <*FedRAMP Assignment: organization-defined subset of privileged 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AU-9 (4) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (PaaS)**  Microsoft Azure implements auditing requirements at the VM level on behalf of PaaS customers.  Microsoft Azure restricts management of audit functionality within Microsoft Azure to the component teams and Azure Security team with approved Azure Standard access. If the audit logs contain EII, the logs are restricted to a defined access group managed by the component team and restricted to need-to-know personnel. These personnel do not have the ability to modify or delete audit records from the central log repositories, and if they disable logging, that action itself is logged.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for restricting the management of customer-controlled audit resources to authorized users. The customer control implementation statement should address the subset of privileged users authorized to manage audit functionality. |

### AU-10 Non-repudiation (H)

The information system protects against an individual (or process acting on behalf of an individual) falsely denying having performed [FedRAMP Assignment: minimum actions including the addition, modification, deletion, approval, sending, or receiving of data].

| AU-10 | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>;* Microsoft Azure | |
| Parameter AU-10: *<FedRAMP Assignment: minimum actions including the addition, modification, deletion, approval, sending, or receiving of data>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AU-10 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (PaaS)**  Microsoft Azure implements auditing requirements at the VM level on behalf of PaaS customers.  Existing two-factor authentication and just-in-time access provide sufficient assurance that privileged actions are restricted to authorized users and that each such action can be associated with the specific user. Events transferred from the Audit Collection Services (ACS) Forwarder to Collector are near real-time. The Collector employs an Immutable collection policy (tamper resilient) to ensure no modification to event logs are made. Alerting and reporting mechanisms are in place to ensure audit events are collected correctly. In the event that errors are detected, a WEC or MDS alert is generated which in turns generates a ticket for the operations team.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (PaaS)**  The customer is responsible for enforcing non-repudiation for customer-deployed resources (to include applications, databases, and software). The customer control implementation statement should address the actions to be covered by non-repudiation (e.g., creating information, sending and receiving messages, approving information) and the techniques employed to support non-repudiation (e.g., digital signatures, digital message receipts).  **Customer Responsibility (IaaS)**  The customer is responsible for enforcing non-repudiation for customer-deployed resources (to include applications, operating systems, databases, and software). The customer control implementation statement should address the actions to be covered by non-repudiation (e.g., creating information, sending and receiving messages, approving information) and the techniques employed to support non-repudiation (e.g., digital signatures, digital message receipts). |

### AU-11 Audit Record Retention (H)

The organization retains audit records for [FedRAMP Assignment: at least one (1) year] 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: <*Customer-defined*>;Microsoft Azure | |
| Parameter AU-11: <*FedRAMP Assignment: at least one (1) year*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AU-11 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (PaaS)**  Microsoft Azure implements auditing requirements at the VM level on behalf of PaaS customers.  Azure implements audit record retention through maintaining all audit records for a minimum of one year. C+E Security has developed an archiving infrastructure to securely store audit records on servers dedicated to archival purposes. The servers are designed to verify the integrity of archived files and allows authorized user to browse to an archive location. Audit records are stored in centralized log servers that are protected against alteration.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (PaaS)**  The customer is responsible for retaining audit records for customer-deployed resources (to include applications, databases, and software) to support security investigations and meet regulatory requirements. The customer control implementation statement should address the retention period and/or corresponding records retention policy.  **Customer Responsibility (IaaS)**  The customer is responsible for retaining audit records for customer-deployed resources (to include applications, operating systems, databases, and software) to support security investigations and meet regulatory requirements. The customer control implementation statement should address the retention period and/or corresponding records retention policy. |

### 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: <*Customer-defined*>;Microsoft Azure | |
| Parameter AU-12(a): <*FedRAMP Assignment: all information system components where audit capability is deployed/available*> | |
| Parameter AU-12(b): *<Customer-defined personnel or roles*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AU-12 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (PaaS)**  Microsoft Azure implements auditing requirements at the VM level on behalf of PaaS customers.  Microsoft Azure 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.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (PaaS)**  The customer is responsible for ensuring all customer-deployed resources (to include applications, databases, and software) have the ability to generate records for the auditable events defined in AU-02.a. The customer control implementation statement should address the system resources with the capability to generate the corresponding audit records.  **Customer Responsibility (IaaS)**  The customer is responsible for ensuring all customer-deployed resources (to include applications, operating systems, databases, and software) have the ability to generate records for the auditable events defined in AU-02.a. The customer control implementation statement should address the system resources with the capability to generate the corresponding audit records. |
| Part b | **Microsoft Azure (PaaS)**  Microsoft Azure implements auditing requirements at the VM level on behalf of PaaS customers.  Microsoft Azure 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 Azure Monitoring and Diagnostics Service (MDS), 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.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for assigning personnel to select audit events for customer-deployed resources. The customer control implementation statement should address the assigned personnel/roles and the customer-deployed resources which will generate the corresponding audit records. |
| Part c | **Microsoft Azure (PaaS)**  Microsoft Azure implements auditing requirements at the VM level on behalf of PaaS customers.  Audit records are captured in Azure Monitoring and Diagnostics Service (MDS), 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.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for generating audit records for the subset of auditable events identified in AU-02.d and content defined in AU-03 for customer-deployed resources. The customer control implementation statement should address how the audit records meet the criteria defined in AU-02 and AU-03. |

#### AU-12 (1) Control Enhancement (H)

The information system compiles audit records from [FedRAMP Assignment: all network, data storage, and computing devices] into a system-wide (logical or physical) audit trail that is time-correlated to within [Assignment: organization-defined level of tolerance for relationship between time stamps of individual records in the audit trail].

| AU-12 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>;* Microsoft Azure | |
| Parameter AU-12 (1)-1: *<FedRAMP Assignment: all network, data storage, and computing devices>* | |
| Parameter AU-12 (1)-2: *<FedRAMP Assignment: organization-defined level of tolerance for relationship between time stamps of individual records in the audit trial>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AU-12 (1) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (PaaS)**  Microsoft Azure implements auditing requirements at the VM level on behalf of PaaS customers.  Microsoft Azure Security correlates audit logs across Microsoft Azure Government. Time stamps are precise at least to the millisecond.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (PaaS)**  The customer is responsible for compiling audit records into a system-wide audit trail for customer-deployed resources (to include applications, databases, and software). The customer control implementation statement should address all customer-deployed resources that provide audit records, and the level of tolerance allowed between time stamps of individual records in the audit trail.  **Customer Responsibility (IaaS)**  The customer is responsible for compiling audit records into a system-wide audit trail for customer-deployed resources (to include applications, operating systems, databases, and software). The customer control implementation statement should address all customer-deployed resources that provide audit records, and the level of tolerance allowed between time stamps of individual records in the audit trail. |

#### AU-12 (3) Control Enhancement (H)

The information system provides the capability for [FedRAMP Assignment: service provider-defined individuals or roles with audit configuration responsibilities] to change the auditing to be performed on [FedRAMP Assignment: all network, data storage, and computing devices] based on [Assignment: organization-defined threat situations] within [Assignment: organization-defined time thresholds].

| AU-12 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>;* Microsoft Azure | |
| Parameter AU-12 (3)-1: *<FedRAMP Assignment:* service provider-defined individuals or roles with audit configuration responsibilities*>* | |
| Parameter AU-12 (3)-2: *<FedRAMP Assignment:* all network, data storage, and computing devices*>* | |
| Parameter AU-12 (3)-3: *<FedRAMP Assignment:* organization-defined threat situations*>* | |
| Parameter AU-12 (3)-4: *<FedRAMP Assignment:* organization-defined time thresholds*>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AU-12 (3) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (PaaS)**  Microsoft Azure implements auditing requirements at the VM level on behalf of PaaS customers.  Microsoft Azure Security personnel are able to update the logging performed by the Monitoring Agent based on changes to the threat environment. The timeframe for these updates is determined by a risk-based assessment.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (PaaS)**  The customer is responsible for providing the capability to extend or limit auditing on customer-deployed resources (to include applications, databases, and software) as necessary to meet organizational requirements. The customer control implementation statement should address the individuals/roles assigned to change auditing levels, the customer-deployed resources generating audit records, the event criteria on which auditing limits or extensions will be based, and the threshold(s) within which those changes must occur.  **Customer Responsibility (IaaS)**  The customer is responsible for providing the capability to extend or limit auditing on customer-deployed resources (to include applications, operating systems, databases, and software) as necessary to meet organizational requirements. The customer control implementation statement should address the individuals/roles assigned to change auditing levels, the customer-deployed resources generating audit records, the event criteria on which auditing limits or extensions will be based, and the threshold(s) within which those changes must occur. |

## Security Assessment and Authorization (CA)

### CA-1 Certification, Authorization, Security Assessment Policy and Procedures (H)

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 annually]; and
   2. Security assessment and authorization procedures [FedRAMP Assignment: at least at least annually or whenever a significant change occurs].

| CA-1 | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer-defined*> | |
| Parameter CA-1(a): <*Customer*-defined personnel or roles> | |
| Parameter CA-1(b)(1): <*FedRAMP Assignment: at least annually*> | |
| Parameter CA-1(b)(2): <*FedRAMP Assignment: at least at least annually or whenever a significant change occurs*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| CA-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for developing, documenting, reviewing, updating, and disseminating security assessment and authorization policy and procedures for the customer’s system. The customer control implementation statement should address the content of the policy (which must include purpose, scope, roles, responsibilities, management commitment, coordination, and compliance), procedures (which must facilitate the implementation of the policies and associated controls), the frequency of review, and the role(s) responsible. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for developing a security assessment plan for the customer-deployed system. The customer control implementation statement should address the scope of the assessment, including: controls and enhancements; assessment procedures; and the assessment environment, team, and roles/responsibilities. |

### 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-2 | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer-defined*> | |
| Parameter CA-2(b): <*FedRAMP Assignment: at least annually*> | |
| Parameter CA-2(d): <*FedRAMP Assignment: individuals or roles to include the FedRAMP Program Management Office (PMO)*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. Date of Authorization, | |

| CA-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for developing a security assessment plan for the customer-deployed system. The customer control implementation statement should address the scope of the assessment, including: controls and enhancements; assessment procedures; and the assessment environment, team, and roles/responsibilities. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for assessing the security controls defined in CA-02.a on customer-deployed resources. The customer control implementation statement should address the implementation, operation, and compliance of the controls, as well as the frequency of assessment. |
| Part c | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for producing a security assessment report. The customer control implementation statement should address documenting the results of the assessment. |
| Part d | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for delivering the security assessment results to the required individuals/roles. The customer control implementation statement should address the individuals or roles the security assessment report (SAR) must be submitted to. |

#### 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-2 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter CA-2(1): <*Customer-defined level of independence. For JAB Authorization, must use an accredited Third Party Assessment Organization (3PAO)>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CA-2 (1) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for employing independent assessors or assessment teams to conduct security control assessments. The customer control implementation statement should address and the level of independence required and the chosen assessor [i.e., an accredited third-party assessment organization (3PAO)]. |

#### 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-2 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter CA-2(2)-1: <*FedRAMP Assignment: at least annually*> | |
| Parameter CA-2(2)-2: *<Selection: announced; unannounced.* *FedRAMP requirement: to include ‘announced’*> | |
| Parameter CA-2(2)-3: < *Selection (one or more): in-depth monitoring; vulnerability scanning; malicious user testing; insider threat assessment; performance/load testing. FedRAMP requirement: to include vulnerability scanning*> | |
| Parameter CA-2(2)-4: <*Customer defined other forms of security assessment*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CA-2 (2) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for the selection of additional testing to be included as part of security control assessments. The customer control implementation statement should address the selected testing mechanisms  (e.g., in-depth monitoring; vulnerability scanning; malicious user testing; insider threat assessment; performance/load testing; and/or customer-defined mechanisms), the frequency of these specialized assessments and whether they are announced or unannounced. |

#### 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-2 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer-defined*> | |
| Parameter CA-2(3)-1: <*Customer-defined information system*> | |
| Parameter CA-2(3)-2: <*FedRAMP Assignment: any FedRAMP Accredited 3PAO* > | |
| Parameter CA-2(3)-3: <*FedRAMP Assignment:* the conditions of the JAB/AO in the FedRAMP Repository> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CA-2 (3) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for accepting assessment results for customer-deployed resources. The customer control implementation statement should address the resources assessed, the external organization performing the assessment, and the requirements that, when met, will result in customer acceptance of the assessment. |

### 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 ‑ CA-3 Authorized Connections

| Authorized Connections Information System Name | Name of Organization CSP Name System Connects To | Role and Name of Person Who Signed Connection Agreement | Name and Date of Interconnection Agreement |
| --- | --- | --- | --- |
| <Authorized Connections System Name> | <Name Org CSP System Connects To> | <Role and Name Signed Connection Agreement> | <Name and Date of Interconnection Agreement> |
| <Authorized Connections System Name> | <Name Org CSP System Connects To> | <Role and Name Signed Connection Agreement> | <Name and Date of Interconnection Agreement> |
| <Authorized Connections System Name> | <Name Org CSP System Connects To> | <Role and Name Signed Connection Agreement> | <Name and Date of Interconnection Agreement> |
| <Authorized Connections System Name> | <Name Org CSP System Connects To> | <Role and Name Signed Connection Agreement> | <Name and Date of Interconnection Agreement> |
| <Authorized Connections System Name> | <Name Org CSP System Connects To> | <Role and Name Signed Connection Agreement> | <Name and Date of Interconnection Agreement> |
| <Authorized Connections System Name> | <Name Org CSP System Connects To> | <Role and Name Signed Connection Agreement> | <Name and Date of Interconnection Agreement> |

| CA-3 | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer-defined*> | |
| Parameter CA-3(c): <*FedRAMP Assignment: At least annually and on input from FedRAMP*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CA-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for authorizing connections from the customer-deployed system to external systems. The customer control implementation statement should address how connections are authorized through the use of Interconnection Security Assessments. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for documenting the details of each interconnection defined in CA-03.a. The customer control implementation statement should address each interconnection's interface characteristics, security requirements, and information communicated. |
| Part c | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for reviewing and updating Interconnection Security Agreements. The customer control implementation statement should address the review and update frequency. |

#### 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-3 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer-defined*> | |
| Parameter CA-3(3)-1: <*Customer-defined unclassified, non-national security system*> | |
| Parameter CA-3(3)-2: <*FedRAMP Assignment: boundary protections which meet Trusted Internet Connection (TIC) 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CA-3 (3) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for prohibiting the direct connection of customer-controlled, unclassified non-national security systems to an external network without the use of appropriate boundary protection devices. The customer control implementation statement should address the unclassified non-national security resources and the boundary protection devices (e.g., routers, firewalls) in place for processing, storing, or transmitting Controlled Unclassified Information (CUI) to an external network. |

#### CA-3 (5) Control Enhancement (H)

The organization employs [FedRAMP Selection: deny-all, permit by exception] policy for allowing [FedRAMP Assignment: any 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-3 (5) | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer-defined*> | |
| Parameter CA-3(5)-1: <*FedRAMP Assignment: deny-all, permit by exception*> | |
| Parameter CA-3(5)-2: <*FedRAMP Assignment: any 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CA-3 (5) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for employing restrictions on external system interconnections. The customer control implementation statement should address the selected policy (e.g., allow-all, deny-by-exception; deny-all, permit-by-exception) and the customer-deployed resources connecting to external 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-5 | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer-defined*> | |
| Parameter CA-5(b): <FedRAMP Assignment: 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CA-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (PaaS)**  The customer is responsible for developing a plan of action and milestones (POA&M) for customer-deployed resources (to include applications, databases, and software). The customer control implementation statement should address the customer's planned remedial actions to correct deficiencies noted during the security assessment (see CA-02) and to reduce/eliminate known vulnerabilities in the system. Additionally, any vulnerabilities found as a result of regular vulnerability scanning (see RA-05) must be included in POA&M reporting.  **Customer Responsibility (IaaS)**  The customer is responsible for developing a plan of action and milestones (POA&M) for customer-deployed resources (to include applications, operating systems, databases, and software). The customer control implementation statement should address the customer's planned remedial actions to correct deficiencies noted during the security assessment (see CA-02) and to reduce/eliminate known vulnerabilities in the system. Additionally, any vulnerabilities found as a result of regular vulnerability scanning (see RA-05) must be included in POA&M reporting. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for updating POA&M items defined in CA-05.a. The customer control implementation statement should address the frequency with which POA&M items will be updated based on findings from security assessments, impact analyses, and continuous monitoring activities. |

### 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-6 | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer-defined*> | |
| Parameter CA-6(c): <FedRAMP Assignment: in accordance with OMB A-130 requirements or when a significant change occurs> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CA-6 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for assigning an authorizing official (AO) for customer-deployed resources. The customer control implementation statement should address the senior-level executive or manager assigned. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for ensuring customer-deployed resources are authorized before operations commence. The customer control implementation statement should address how the AO has authorized the customer-deployed resources for processing. |
| Part c | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for updating the security authorization for customer-deployed resources. The customer control implementation statement should address the frequency in which the authorization will be updated. |

### 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-7 | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer-defined*> | |
| Parameter CA-7(a): *<Customer-defined metrics>* | |
| Parameter CA-7(b)-1: *<Customer-defined frequencies>* | |
| Parameter CA-7(b)-2: *<Customer-defined frequencies>* | |
| Parameter CA-7(g)-1: *<FedRAMP Assignment:* to meet Federal and FedRAMP requirements*>* | |
| Parameter CA-7(g)-2: *<Customer-defined frequency>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CA-7 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (PaaS)**  The customer is responsible for developing a continuous monitoring strategy and implementing a continuous monitoring program for customer-deployed resources (to include applications, databases, and software). The customer control implementation statement should address the metrics to be monitored.  FedRAMP Requirement: The customer is responsible for performing vulnerability scans on customer-deployed web applications, and databases, at least monthly.  **Customer Responsibility (IaaS)**  The customer is responsible for developing a continuous monitoring strategy and implementing a continuous monitoring program for customer-deployed resources (to include applications, operating systems, databases, and software). The customer control implementation statement should address the metrics to be monitored.  FedRAMP Requirement: The customer is responsible for performing vulnerability scans on customer-deployed operating systems, web applications, and databases, at least monthly. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (PaaS)**  The customer is responsible for continuously monitoring customer-deployed resources and performing supporting assessments of that monitoring activity. The customer control implementation statement should address the frequency with which monitoring and supporting assessments will be performed.  FedRAMP Requirement: The customer is responsible for performing vulnerability scans on customer-deployed web applications and databases, at least monthly.  **Customer Responsibility (IaaS)**  The customer is responsible for continuously monitoring customer-deployed resources and performing supporting assessments of that monitoring activity. The customer control implementation statement should address the frequency with which monitoring and supporting assessments will be performed.  FedRAMP Requirement: The customer is responsible for performing vulnerability scans on customer-deployed operating systems, web applications, and databases, at least monthly. |
| Part c | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for ongoing security assessments. The customer control implementation statement should address how these assessments are in accordance with the customer's continuous monitoring strategy.  FedRAMP Requirement: The customer is responsible for having an independent assessor perform vulnerability scans, at least annually. The customer control implementation statement should address frequency with which scans are performed. |
| Part d | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for ongoing security status monitoring of the metrics defined in CA-07.a. The customer control implementation statement should address how this monitoring is in accordance with the customer's continuous monitoring strategy. |
| Part e | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for correlating and analyzing security-related information generated by assessments and monitoring of customer-deployed resources. The customer control implementation statement should address how this information is correlated and analyzed. |
| Part f | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for responding to the results of the analysis defined in CA-07.e. The customer control implementation statement should address under which conditions each response action should be taken (e.g., if a new vulnerability is found in the system, a POA&M item should be opened). |
| Part g | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for reporting the security status of customer-deployed resources. The customer control implementation statement should address which personnel/roles will be notified of the security status and the frequency with which reporting will occur. |

CA-7 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-7 Req. | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CA-7 What is the solution and how is it implemented? | |
| --- | --- |
| Req. 1 | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (PaaS)**  The customer is responsible for continuously monitoring customer-deployed resources and performing supporting assessments of that monitoring activity. The customer control implementation statement should address the frequency with which monitoring and supporting assessments will be performed.  FedRAMP Requirement: The customer is responsible for performing vulnerability scans on customer-deployed web applications and databases, at least monthly.  **Customer Responsibility (IaaS)**  The customer is responsible for continuously monitoring customer-deployed resources and performing supporting assessments of that monitoring activity. The customer control implementation statement should address the frequency with which monitoring and supporting assessments will be performed.  FedRAMP Requirement: The customer is responsible for performing vulnerability scans on customer-deployed operating systems, web applications, and databases, at least monthly. |
| Req. 2 | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (PaaS)**  The customer is responsible for developing a continuous monitoring strategy and implementing a continuous monitoring program for customer-deployed resources (to include applications, databases, and software). The customer control implementation statement should address the metrics to be monitored.  FedRAMP Requirement: The customer is responsible for performing vulnerability scans on customer-deployed web applications and databases, at least monthly.  **Customer Responsibility (IaaS)**  The customer is responsible for developing a continuous monitoring strategy and implementing a continuous monitoring program for customer-deployed resources (to include applications, operating systems, databases, and software). The customer control implementation statement should address the metrics to be monitored.  FedRAMP Requirement: The customer is responsible for performing vulnerability scans on customer-deployed operating systems, web applications, and databases, at least monthly. |
| Req. 3 | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (PaaS)**  The customer is responsible for ongoing security assessments. The customer control implementation statement should address how these assessments are in accordance with the customer's continuous monitoring strategy.  FedRAMP Requirement: The customer is responsible for having an independent assessor perform vulnerability scans, at least annually. The customer control implementation statement should address frequency with which scans are performed.  **Customer Responsibility (IaaS)**  The customer is responsible for ongoing security assessments. The customer control implementation statement should address how these assessments are in accordance with the customer's continuous monitoring strategy.  FedRAMP Requirement: The customer is responsible for having an independent assessor perform vulnerability scans, at least annually. The customer control implementation statement should address frequency with which scans are performed. |

#### 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-7 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter CA-7(1): *<Customer*-defined level of independence> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CA-7 (1) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for employing independent assessors or assessment teams to monitor security controls for customer-deployed resources on an ongoing basis. The customer control implementation statement should address and the level of independence required and the chosen assessor [i.e., an accredited third-party assessment organization (3PAO)]. |

#### CA-7 (3) Control Enhancement (H)

The organization employs trend analyses to determine if security control implementations, the frequency of continuous monitoring activities, and/or the types of activities used in the continuous monitoring process need to be modified based on empirical data.

| CA-7 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CA-7 (3) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for employing continuous monitoring trend analyses. The customer control implementation statement should address the process to determine if security control implementations, the frequency of continuous monitoring activities, and/or the types of activities used in the continuous monitoring process need to be modified based on empirical data obtained from trend analyses. |

### 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-8 | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter CA-8-1: <FedRAMP Assignment: at least annually> | |
| Parameter CA-8-2: *<Customer-defined information systems or 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CA-8 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for conducting penetration testing for customer-deployed resources. The customer control implementation statement should address the frequency of testing and the resources tested. |

#### 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-8 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CA-8 (1) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for employing an independent agent or team to perform penetration testing on customer-deployed resources (note that this may be the 3PAO used for recurring assessments, or it may be a different independent assessor). The customer control implementation statement should address the selected independent agent/team and the resources to be tested. |

### 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: *<Customer-defined>* | |
| Parameter CA-9(a): *<Customer-defined information system components or classes of 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CA-9 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for authorizing internal connections across customer-deployed resources (e.g., system connections to VMs). The customer control implementation statement should address the customer-deployed resources or classes of resources authorized to connect internally. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for documenting the details of each internal connection between the classes/resources defined in CA-09.a. The customer control implementation statement should address each internal connection's interface characteristics, security requirements, and information communicated. |

## Configuration Management (CM)

### CM-1 Configuration Management Policies and Procedures (H)

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 annually]; and
   2. Configuration management procedures [FedRAMP Assignment: at least annually or whenever a significant change occurs].

| CM-1 | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter CM-1(a): *<Customer-defined personnel or roles>* | |
| Parameter CM-1(b)(1): *<FedRAMP Assignment: at least annually>* | |
| Parameter CM-1(b)(2): *<FedRAMP Assignment: at least annually or whenever a significant change occurs>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CM-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for developing, documenting, reviewing, updating, and disseminating configuration management policy and procedures for customer-deployed resources. The customer control implementation statement should address the content of the policy (which must include purpose, scope, roles, responsibilities, management commitment, coordination, and compliance), procedures (which must facilitate the implementation of the policies and associated controls), the frequency of review, and the role(s) responsible. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for developing, documenting, reviewing, updating, and disseminating configuration management policy and procedures for customer-deployed resources. The customer control implementation statement should address the content of the policy (which must include purpose, scope, roles, responsibilities, management commitment, coordination, and compliance), procedures (which must facilitate the implementation of the policies and associated controls), the frequency of review, and the role(s) responsible. |

### 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-2 | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>*;Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CM-2 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (PaaS)**  Microsoft Azure implements portions of configuration management controls for operating systems leveraged by PaaS customers.  Customers are responsible for implementing this control for any customer applications.  Microsoft Azure reviews and updates configuration settings and baseline configurations of hardware, software and network devices annually. Changes are developed, tested, and approved prior to entering the production environment from a development and/or test environment.  Changes to the Microsoft Azure component/role baseline configurations are deployed to the production environment using the change and release management process. The change and release management process validates that the build moves from one environment to the other with designated sign-offs by appropriate Microsoft Azure component team personnel. Access to migrate changes to production is restricted in accordance with CM-5.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (PaaS)**  The customer is responsible for a baseline configuration of customer-deployed resources (to include applications, databases, and software). The customer control implementation statement should address the organization’s process for developing, documenting, and maintaining the baseline configuration.  **Customer Responsibility (IaaS)**  The customer is responsible for a baseline configuration of customer-deployed resources (to include applications, operating systems, databases, and software). The customer control implementation statement should address the organization’s process for developing, documenting, and maintaining the baseline configuration. |

#### CM-2 (1) Control Enhancement (H)

The organization reviews and updates the baseline configuration of the information system:

1. [FedRAMP Assignment: at least annually or when a significant change occurs];
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) (a) Additional FedRAMP Requirements and Guidance:

Guidance: Significant change is defined in NIST Special Publication 800-37 Revision 1, Appendix F, Page F-7.

| CM-2 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>*;Microsoft Azure | |
| Parameter CM-2(1)(a): *<FedRAMP Assignment: at least annually or when a significant change occurs>* | |
| Parameter CM-2(1)(b): *<FedRAMP Assignment: to include when directed by the JAB>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CM-2 (1) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (PaaS)**  Microsoft Azure implements portions of configuration management controls for operating systems leveraged by PaaS customers.  The Microsoft Azure RDOS team thoroughly reviews and updates the baseline configuration based on new security configurations or changes to existing security configurations of the Microsoft Azure OS and Microsoft Azure components annually as part of the change and release management process.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (PaaS)**  The customer is responsible for reviewing and updating the baseline configuration of customer-deployed resources (to include applications, databases, and software). The customer control implementation statement should address how often the baseline configuration is reviewed and updated.  **Customer Responsibility (IaaS)**  The customer is responsible for reviewing and updating the baseline configuration of customer-deployed resources (to include applications, operating systems, databases, and software). The customer control implementation statement should address how often the baseline configuration is reviewed and updated. |
| Part b | **Microsoft Azure (PaaS)**  Microsoft Azure implements portions of configuration management controls for operating systems leveraged by PaaS customers.  The Microsoft Azure RDOS team reviews and updates the OS and component baseline configurations when required due to a significant change. Changes from USCYBERCOM tactical orders/directives can be accommodated. However, analysis is required to determine if any particular directive is applicable to the Microsoft Azure services. There is a reasonable probability that any particular directive will be not applicable. Microsoft internal components are specifically engineered for its operations and do not rely on 3rd party applications. They are further isolated from direct external connections. They must be further tested to ensure that there is no detrimental impact to the baseline configurations and that the associated vulnerability is not already accommodated by compensating/mitigating controls. All changes must go through the deployment process, as defined in CM-3. Changes may include, but are not limited to the following:   * Installation of a new or upgraded operating system, middleware component, or application; * Modifications to system ports, protocols, or services; * Installation of a new or upgraded hardware platform; * Modifications to cryptographic modules or services; or * Modifications to security controls.   Additionally, the baseline configurations may be reviewed and updated based on significant change to the Microsoft Azure environment which may include, but is not limited to the following:   * Moving to a new facility; * Adding new core missions or business functions; * Acquiring specific and credible threat information that the organization is being targeted by a threat source; or * Establishing new/modified laws, directives, policies, or regulations.   **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for reviewing and updating the baseline configuration of customer-deployed resources when required. The customer control implementation statement should address any organization-defined circumstances that necessitate a baseline configuration review or update. The Joint Authorization Board (JAB) or USCYBERCOM may influence organization-defined circumstances. |
| Part c | **Microsoft Azure (PaaS)**  Microsoft Azure implements portions of configuration management controls for operating systems leveraged by PaaS customers.  The Microsoft Azure RDOS team reviews and updates the applicable baseline configurations as part of the new OS or component-specific release and upgrades. Azure publishes new OS configuration baselines every 30 days, internally. The new baselines are intended to be implemented across Azure in as near to real time as possible.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for reviewing and updating the baseline configuration of customer-deployed resources when required. The customer control implementation statement should address how the baseline configuration is reviewed and updated when installations and upgrades occur. |

#### 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-2 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>*; Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CM-2 (2) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (PaaS)**  Microsoft Azure stores baseline configuration information in Source Depot and Git. Both of these are automated mechanisms that allow Microsoft Azure to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for employing automated mechanisms to maintain the baseline configuration of customer-deployed resources. The customer control implementation statement should address the automated mechanisms used to maintain an up-to-date, complete, accurate, and readily available baseline configuration. |

#### CM-2 (3) Control Enhancement (H)

The organization retains [FedRAMP Assignment: the previously approved baseline configuration of IS components] to support rollback.

| CM-2 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>*;Microsoft Azure | |
| Parameter CM-2(3): *<FedRAMP Assignment: the previously approved baseline configuration of IS 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CM-2 (3) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (PaaS)**  Microsoft Azure implements portions of configuration management controls for operating systems leveraged by PaaS customers.  Microsoft Azure has implemented procedures for at least the most recent previous version of the baseline configuration within Source Depot or Git in the event information systems need to roll back to a stable version.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for retaining previous versions of baseline configurations for customer-deployed resources. The customer control implementation statement should address the number of previous configuration versions to retain and the required retention period. |

#### 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: Microsoft Azure | |
| Parameter CM-2(7)(a)-1: *<Customer-defined information systems, system components, or devices>* | |
| Parameter CM-2(7)(a)-2: *<Customer-defined configurations>* | |
| Parameter CM-2(7)(b): *<Customer-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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CM-2 (7) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure customer content is never stored outside of Microsoft Azure, which is physically located within the continental United States. Microsoft Azure personnel do not travel with devices contained within the Microsoft Azure inventory. As such, this control is not applicable to Microsoft Azure.  **Customer Responsibility (IaaS/PaaS)**  There are no customer-controlled physical resources within the scope of systems deployed on Azure; all physical resource protection controls are implemented and managed by Microsoft. This control is inherited from Azure. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure customer content is never stored outside of Microsoft Azure and Microsoft Azure personnel do not travel with devices contained within the Microsoft Azure inventory, thus this control is not applicable.  **Customer Responsibility (IaaS/PaaS)**  There are no customer-controlled physical resources within the scope of systems deployed on Azure; all physical resource protection controls are implemented and managed by Microsoft. This control is inherited from Azure. |

### 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: *<Customer-defined>*;Microsoft Azure | |
| Parameter CM-3(e): *<Customer-defined time period>* | |
| Parameter CM-3(g)-1: *<FedRAMP Assignment: 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.>* | |
| Parameter CM-3(g)-2: *<FedRAMP Assignment: Selection (one or more)>* | |
| Parameter CM-3(g)-3: *<Customer-defined frequency>* | |
| Parameter CM-3(g)-4: *<Customer-defined configuration change conditions>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CM-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (PaaS)**  Microsoft Azure implements portions of configuration management controls for operating systems leveraged by PaaS customers.  Changes to operational systems, other than security patches, can only be made when there is a valid business reason (e.g., a planned upgrade to the system). Changes implemented within the production environment are categorized into RFC types to appropriately schedule, align resources, and provide change metrics back into the change process for continuous improvement. In general, the Microsoft Azure services teams use the following change types: Major Release, Minor Release, and Revision Release.  Naming convention for build releases varies by service teams and the specific processes required for the release are specified in the service team specific change management process documents.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (PaaS)**  The customer is responsible for determining what types of changes to customer-deployed resources (to include applications, databases, and software) are configuration-controlled. The customer control implementation statement should address the changes that are controlled by a configuration.  **Customer Responsibility (IaaS)**  The customer is responsible for determining what types of changes to customer-deployed resources (to include applications, operating systems, databases, and software) are configuration-controlled. The customer control implementation statement should address the changes that are controlled by a configuration. |
| Part b | **Microsoft Azure (PaaS)**  Microsoft Azure implements portions of configuration management controls for operating systems leveraged by PaaS customers.  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.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for reviewing proposed configuration-controlled changes to customer-deployed resources. The customer control implementation statement should address the approval/rejection process for configuration changes, and how security impact is taken into consideration for proposed changes. |
| Part c | **Microsoft Azure (PaaS)**  Microsoft Azure implements portions of configuration management controls for operating systems leveraged by PaaS customers.  Microsoft Azure service teams use TFS, Source Depot and Git to document evidence of approval and track all changes.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for documenting configuration-controlled changes associated with customer-deployed resources (see CM-03.b). The customer control implementation statement should address the documentation of configuration change decisions. |
| Part d | **Microsoft Azure (PaaS)**  Microsoft Azure implements portions of configuration management controls for operating systems leveraged by PaaS customers.  The change tools discussed in part c of this control ensure that configuration-controlled changes are implemented after they are approved by tracking the change through implementation.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for implementing configuration-controlled changes approved in CM-03.b. The customer control implementation statement should address how approved changes are implemented to customer-deployed resources. |
| Part e | **Microsoft Azure (PaaS)**  Microsoft Azure implements portions of configuration management controls for operating systems leveraged by PaaS customers.  Approval of the changes is documented in the change management release to operations hand-off criteria document.  Depending on the type of change, the evidence of release approval may be documented in the Incident Management system, in the TFS tickets, or in the RTO tool tickets. These change management records are retained for a minimum of 90 days.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (PaaS)**  The customer is responsible for retaining a record of configuration-controlled changes to customer-deployed resources. The customer control implementation statement should address the retention period for these records. |
| Part f | **Microsoft Azure (PaaS)**  Microsoft Azure implements portions of configuration management controls for operating systems leveraged by PaaS customers.  The tools outlined in part c of this control provide an auditing capability to any changes to the baselines or configuration changes within the tools. Microsoft Azure uses Source Depot and Git as the versioning systems for software code. Both of these tools track the identity of the person who checks code out, the time of the change, and what changes are made to what files. Software and hardware changes are tracked through TFS. Cloud Engineering Systems team manages the software updates, and hardware changes with MSIT. Cloud Engineering Systems team owns the content and policies and the hardware changes are implemented by MSIT.  In addition, an annual external audit is performed on the Microsoft Azure change management process as part of annual Microsoft Azure security assessment. As part of the audit, a sample of changes are selected and reviewed to determine if the change management process is consistently being followed.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for auditing and reviewing configuration changes. The customer control implementation statement should address the process for auditing and reviewing activities associated with configuration-controlled changes to customer-deployed resources. |
| Part g | **Microsoft Azure (PaaS)**  Microsoft Azure implements portions of configuration management controls for operating systems leveraged by PaaS customers.  All changes, except pre-approved changes, to the Microsoft Azure production environment must go through CAB approval. Each service team has an internal CAB with designated roles; these service team CABs meet at least monthly, or as needed.  Pre-approved changes: There are a set of CAB pre-approved changes which do not require additional explicit approval for release. These are standard procedures/common tasks that are documented and are confirmed to be safe to perform without going through the formal change management process. A complete list of pre-approved change types is maintained by the RDRELPM on the release management SharePoint site. Examples of pre-approved Change Types are Create Certificate and Create Stage XStore Account.  For all Microsoft Azure components, Microsoft works with FedRAMP. Specifically, Microsoft participates in weekly meetings with the FedRAMP PMO and the assigned ISSO to communicate major changes to or developments in the Microsoft Azure environment. Escalation to the FedRAMP JAB is at the discretion of the PMO.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for coordinating and providing oversight for configuration change control activities. The customer control implementation statement should address the change control element assigned (e.g., committee, board), and the frequency and/or change condition(s) under which the change control element convenes. |

#### CM-3 (1) Control Enhancement (H)

The organization employs automated mechanisms to:

1. Document proposed changes to the information system;
2. Notify [Assignment: organization-defined configuration management approval authorities] of proposed changes to the information system and request change approval;
3. Highlight proposed changes to the information system that have not been approved or disapproved by [FedRAMP Assignment: organization agreed upon time period];
4. Prohibit changes to the information system until designated approvals are received;
5. Document all changes to the information system; and
6. Notify [FedRAMP Assignment: organization-defined configuration management approval authorities] when approved changes to the information system are completed.

| CM-3 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter CM-3 (1)(b): *<Customer-defined configuration management approval authorities>* | |
| Parameter CM-3 (1)(c): *<FedRAMP Assignment: organization agreed upon time period>* | |
| Parameter CM-3 (1)(f): *<FedRAMP Assignment: organization-defined configuration management approval authorities>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CM-3 (1) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for employing automated mechanisms to document proposed changes (see CM-03.b). The customer control implementation statement should address the mechanism(s) in place to document proposed changes to customer-deployed resources. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for employing an automated mechanism to route and request approval for proposed changes to customer-deployed resources. The customer control implementation statement should address the mechanism to notify the approval authorities identified in CM-03.g that a change request is awaiting approval. |
| Part c | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for employing an automated mechanism to highlight unreviewed change proposals. The customer control implementation statement should address the mechanism in place to highlight requests, as well as the time period at which unreviewed changes to customer-deployed resources will be highlighted. |
| Part d | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for employing an automated mechanism to prohibit the implementation of unapproved changes to customer-deployed resources. The customer control implementation statement should address the mechanism in place to prevent changes from being deployed until approval is received. |
| Part e | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for employing an automated mechanism to document all implemented changes to customer-deployed resources. The customer control implementation statement should address the mechanism in place to document changes. |
| Part f | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for employing an automated mechanism to provide notifications when approved changes to customer-deployed resources are completed. The customer control implementation statement should address the notification mechanism in place, and the personnel to be notified. |

#### CM-3 (2) Control Enhancement (M)(H)

The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.

| CM-3 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CM-3 (2) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for testing, validating, and documenting changes to customer-deployed resources before implementation. The customer control implementation statement should address the process used to test, validate, and document changes before they are deployed. |

#### CM-3 (4) Enhancement (H)

The organization requires an information security representative to be a member of the [FedRAMP Assignment: configuration control board (CCB) or similar (as defined in CM-3)].

| CM-3 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter CM-3 (4): *<FedRAMP Assignment: configuration control board (CCB) or similar (as defined in CM-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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CM-3 (4) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for assigning an information security representative to be a member of the change control element defined in CM-03.g. The customer control implementation statement should address the assigned security representative. |

#### CM-3 (6) Enhancement (H)

The organization ensures that cryptographic mechanisms used to provide [FedRAMP Assignment: all security safeguards that rely on cryptography] are under configuration management.

| CM-3 (6) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter CM-3 (6): *<FedRAMP Assignment: all security safeguards that rely on cryptography>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CM-3 (6) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for ensuring that cryptographic mechanisms are under configuration management. The customer control implementation statement should address the cryptographic mechanisms, the organization-defined security safeguards they provide, and how the processes and procedures in place to effectively manage changes to those mechanisms. |

### 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-4 | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>*;Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CM-4 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (PaaS)**  Microsoft Azure implements portions of configuration management controls for operating systems leveraged by PaaS customers.  As part of the SDL process, Microsoft Azure analyzes software and hardware changes to determine potential security impacts prior to change implementation. Changes are required to be documented, tested, and approved by appropriate personnel.  Additionally, for all asset types, changes are analyzed as part of the standard change management process, both prior to and after implementation, to verify that what was modified resulted in expected output. Information security impact analysis is performed and reviewed by each service team using their individual processes prior to the change being implemented.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for analyzing proposed changes to customer-deployed resources. The customer control implementation statement should address the process used to analyze changes to determine potential security impacts prior to implementation. |

#### CM-4 (1) Control Enhancement (H)

The organization analyzes changes to the information system in a separate test environment before implementation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.

| CM-4 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CM-4 (1) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for analyzing proposed changes to customer-deployed resources in a test environment before implementation in an operational environment. The customer control implementation statement should address how the test environment analysis looks for security impacts due to flaws, weaknesses, incompatibility, or intentional malice. |

### 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-5 | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>*;Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CM-5 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (PaaS)**  Microsoft Azure implements portions of configuration management controls for operating systems leveraged by PaaS customers.  Microsoft Azure service teams define, document, approve, and enforce logical access restrictions associated with changes by using role-based access control (RBAC) enforced by Active Directory (AD). All accounts created in support of Microsoft Azure are role-based. Service team personnel request access to, and if approved, are placed in the appropriate security groups according to their roles for supporting the system and using the principles of least privilege.  Access to the production environment is only allowed to members of specific security groups after approval. A subset of service team personnel have undergone background checks and have gone through the approval process for Operations-level read access to production, used during critical incident escalations.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for enforcing access restrictions when making changes to customer-deployed resources. The customer control implementation statement should address how logical access associated with change control is defined, documented, approved, and enforced. |

#### CM-5 (1) Control Enhancement (M) (H)

The information system enforces access restrictions and supports auditing of the enforcement actions.

| CM-5 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>*;Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CM-5 (1) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (PaaS)**  Microsoft Azure implements portions of configuration management controls for operating systems leveraged by PaaS customers.  Service teams use Active Directory (AD) and Just-In-Time access (JIT) to control access to change functions. AD defines the access that is available, and JIT provides time-limited permission elevation when users actually need to use that access. AD is discussed in greater detail in AC-2 and AC-3. AD and JIT are automated, and actions taken (account creation, change, disabling, removal for AD; account elevation for JIT) are automatically audited as discussed in AU-2 and AU-3.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for enforcing the access restrictions defined in CM-05. The customer control implementation statement should address how access restrictions are enforced, and how auditing of enforcement actions is supported. |

#### CM-5 (2) Control Enhancement (H)

The organization reviews information system changes [FedRAMP Assignment: at least every thirty (30) days] and [Assignment: organization-defined circumstances] to determine whether unauthorized changes have occurred.

| CM-5 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter CM-5 (2)-1: *<FedRAMP Assignment: at least every thirty (30) days>* | |
| Parameter CM-5 (2)-2: *<Customer-defined circumstances>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CM-5 (2) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for reviewing changes to customer-deployed resources to determine whether unauthorized changes have occurred. The customer control implementation statement should address the frequency and circumstances that would necessitate a review. |

#### 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-5 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>*; Microsoft Azure | |
| Parameter CM-5(3): *<FedRAMP Assignment: organization-defined software and firmware 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CM-5 (3) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (PaaS)**  Microsoft Azure implements portions of configuration management controls for operating systems leveraged by PaaS customers.  In accordance with Microsoft Security Policy, all software installed within Microsoft Azure must have a valid signature.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for restricting the installation of software and firmware. The customer control implementation statement should address how the organization prevents installations without verification that the software/firmware has been digitally signed using a certificate that is recognized and approved by the customer. |

#### 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: *<Customer-defined>*; Microsoft Azure | |
| Parameter CM-5(5)(b): *<FedRAMP Assignment: at least quarterly>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CM-5 (5) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (PaaS)**  Microsoft Azure implements portions of configuration management controls for operating systems leveraged by PaaS customers.  Microsoft Azure developers/integrators do not have access to any of the Microsoft Azure production environments to change hardware, software, or firmware components. Developers and integrators are responsible for developing the code, generating the builds, performing integration testing, and managing deployments. Microsoft Azure limits privileges to release software and configuration changes to production to authorized personnel; only the designated approvers (leads, managers, or PMs) can approve changes to Production, and the Development and Operations teams (DevOps model) deploy the changes.  As mentioned above in CM-5, segregation of duties is established on all critical functions within Microsoft Azure’s production environment, to minimize the risk of unauthorized changes to productions systems. As such, access to make changes to the production environment is limited to authorized members in the Development and Operations teams (DevOps model).  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for limiting privileges to make changes within customer-deployed production or operational environments. The customer control implementation statement should address how privileges to change production/operation environments are limited. This can include defining who has access to which privileges and how privileges are separated. |
| Part b | **Microsoft Azure (PaaS)**  Microsoft Azure implements portions of configuration management controls for operating systems leveraged by PaaS customers.  Microsoft Azure service teams review developer/integrator access at least quarterly, consistent with normal account review processes.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for reviewing and reevaluating privileges defined in CM-05(05).a. The customer control implementation statement should address how often privileges are reviewed and re-evaluated. |

### 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: *<Customer-defined>*;Microsoft Azure | |
| Parameter CM-6(a)-1: *<FedRAMP Assignment: 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>* | |
| Parameter CM-6(a)-2: *<FedRAMP Assignment: The service provider shall ensure that checklists for configuration settings are Security Content Automation Protocol (SCAP) (*[*http://scap.nist.gov/*](http://scap.nist.gov/)*) validated or SCAP compatible (if validated checklists are not available)>* | |
| Parameter CM-6(c)-1: *<Customer-defined information system components>* | |
| Parameter CM-6(c)-2: *<Customer-defined 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CM-6 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (PaaS)**  Microsoft Azure implements portions of configuration management controls for operating systems leveraged by PaaS customers.  Input to the configuration settings for OS images and scripts used in Microsoft Azure come from product architecture and security analysis as well as direction from Microsoft Azure Security to ensure a secure defense-in-depth deployment of technologies; Microsoft Azure uses the USGCB and CIS Benchmarks in development of the base images. Microsoft Azure performs security impact analysis for all the new features and code changes.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for establishing and documenting configuration settings for customer-deployed resources (to include applications, databases, and software) that reflect the most restrictive mode consistent with operational requirements. The customer control implementation statement should address the IT products and the customer-defined security configuration checklists assigned to them. |
| Part b | **Microsoft Azure (PaaS)**  Microsoft Azure implements portions of configuration management controls for operating systems leveraged by PaaS customers.  Mandatory configuration settings are implemented on each Microsoft Azure component as specified in the corresponding mandatory configuration settings/baseline documentation for each component, which are established as described in part a of this control. New security configurations or changes to existing security configurations of software components are thoroughly reviewed and tested in DEV before entering the production environment as part of the change and release management process.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for implementing the configuration settings defined in CM-06.a. The customer control implementation statement should address the process for implementing configuration settings. |
| Part c | **Microsoft Azure (PaaS)**  Microsoft Azure implements portions of configuration management controls for operating systems leveraged by PaaS customers.  There are currently no exceptions to the mandatory configuration settings in Microsoft Azure, as all Microsoft Azure components are running one of the approved builds. In the case of an exception, the exception would be documented through the change management process and approved by the CAB.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for identifying, documenting, and approving any deviations from established configuration settings for customer-deployed resources. The customer control implementation statement should address the resources requiring deviation and the operational requirements on which the deviations are based. |
| Part d | **Microsoft Azure (PaaS)**  Microsoft Azure implements portions of configuration management controls for operating systems leveraged by PaaS customers.  All configuration changes are limited to the specific personnel responsible for the component and are captured in audit logs. In addition, vulnerability scans are run to assist in determining the effectiveness of the configuration settings on the applications and servers.  Only certain individuals have the privileges to make changes to the configuration of the system based on an approved access model that requires establishing business justification for the membership. If an unauthorized person attempts to make changes, the system 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 Microsoft Azure 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.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for monitoring and controlling changes to the configuration settings in accordance with organization policies and procedures. The customer control implementation statement should address how changes are controlled and monitored. |

#### 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-6 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>*;Microsoft Azure | |
| Parameter CM-6(1): *<Customer-defined 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CM-6 (1) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (PaaS)**  Microsoft Azure implements portions of configuration management controls for operating systems leveraged by PaaS customers.  Microsoft Azure service teams use Active Directory Group Policy Objects (GPOs) as an automated mechanism to centrally manage, apply, and verify security configuration settings. For virtual machines that are not domain-joined (i.e. those in the Microsoft Azure virtual environment), Microsoft Azure uses OS images that already have the appropriate settings configured at deployment.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for employing automated mechanisms to centrally manage, apply, and verify configuration settings for customer-deployed resources. The customer control implementation statement should address the resources configured. |

#### CM-6 (2) Control Enhancement (H)

The organization employs [Assignment: organization-defined security safeguards] to respond to unauthorized changes to [Assignment: organization-defined configuration settings].

| CM-6 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter CM-6 (2)-1: *<Customer-defined security safeguards>* | |
| Parameter CM-6 (2)-2: *<Customer-defined configuration settings>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CM-6 (2) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for employing security safeguards to respond to unauthorized changes to configuration settings for customer-deployed resources. The customer control implementation statement should address the safeguards in place to prevent unauthorized changes, as well as the configuration settings that these safeguards apply to. |

### 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: *<Customer-defined>*;Microsoft Azure | |
| Parameter CM-7(b): *<FedRAMP Assignment: United States Government Configuration Baseline (USGCB). 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>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. Date of Authorization, | |

| CM-7 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (PaaS)**  Microsoft Azure implements portions of configuration management controls for operating systems leveraged by PaaS customers.  Microsoft Azure uses a combination of USGCB guidance and CIS Benchmarks for development of all base operating system images, configuration scripts, and configuration files deployed within the system. These baselines help to ensure that only essential functions, ports, protocols, and services are enabled for each server role.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for configuring customer-deployed resources to only provide essential capabilities (e.g., disabling extraneous services that may be provided by default, using a system for a single function rather than a system supporting multiple functions). The customer control implementation statement should address the process used to ensure that customer systems only provides essential capabilities. |
| Part b | **Microsoft Azure (PaaS)**  Microsoft Azure implements portions of configuration management controls for operating systems leveraged by PaaS customers.  Base operating system images are developed using USGCB guidance and CIS benchmarks. These base images include essential functions, ports, protocols, and services. All other functions, ports, protocols, and services are disabled by default. Service teams must go through an approval process to have a port opened, or a function, protocol, or service enabled.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for prohibiting or restricting the use of specific functions, ports, protocols, and/or services. The customer control implementation statement should address the identified functions, ports, protocols, and/or services that are prohibited and/or restricted to provide least functionality. |

#### 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: *<Customer-defined>*;Microsoft Azure | |
| Parameter CM-7(1)(a): *<FedRAMP Assignment: at least monthly>* | |
| Parameter CM-7(1)(b): *<Customer-defined functions, ports, protocols, and services within the information system deemed to be unnecessary and/or nonsecure>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CM-7 (1) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (PaaS)**  Microsoft Azure implements portions of configuration management controls for operating systems leveraged by PaaS customers.  Microsoft Azure software and hardware configurations and Access Control Lists (ACLs) are reviewed at least monthly to identify any unnecessary or unsecure functions, ports, protocols, and services.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for reviewing customer-deployed resources (to include applications, databases, and software) to identify unnecessary and/or unsecure functions, ports, protocols, and services. The customer control implementation statement should address the frequency of review.  **Customer Responsibility (IaaS)**  The customer is responsible for reviewing customer-deployed resources (to include applications, operating systems, databases, and software) to identify unnecessary and/or unsecure functions, ports, protocols, and services. The customer control implementation statement should address the frequency of review. |
| Part b | **Microsoft Azure (PaaS)**  Microsoft Azure implements portions of configuration management controls for operating systems leveraged by PaaS customers.  Any function, port, protocol, or service identified as unnecessary or unsecure during the review process is disabled.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for disabling functions, ports, protocols, and services that have been deemed to be unnecessary or unsecure. The customer control implementation statement should address how functions, ports, protocols, and services found during the review process defined in CM-07(01).a are disabled. |

#### 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-7 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>*;Microsoft Azure | |
| Parameter CM-7(2): *<Customer-defined policies regarding software program usage and restrictions;* rules authorizing the terms and conditions of software program usage*>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CM-7 (2) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (PaaS)**  Microsoft Azure implements portions of configuration management controls for operating systems leveraged by PaaS customers.  As part of the SDL process, teams provide lists of software they use to provide the service. These lists go through Security and Privacy reviews. Installed software is monitored using ASM. If unauthorized software installation is detected, the Security team responds in accordance with SI-7(7).  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for preventing program execution in accordance with customer-defined software program usage policies. The customer control implementation statement should address the requirement that program execution is prevented in accordance with organization-defined policies regarding software program usage and restrictions, and/or rules authorizing the terms and conditions of software program usage. |

#### CM-7 (5) Control Enhancement (H)

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 quarterly or when there is a change].

| CM-7 (5) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>*;Microsoft Azure | |
| Parameter CM-7(5)(a): *<Customer-defined software programs authorized to execute on the information system>* | |
| Parameter CM-7(5)(b): *<FedRAMP Assignment: at least quarterly 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CM-7 (5) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (PaaS)**  Microsoft Azure implements portions of configuration management controls for operating systems leveraged by PaaS customers.  Microsoft Azure identifies software authorized to execute within Microsoft Azure 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 Microsoft Azure. Microsoft Azure uses Azure Security Monitoring (ASM) to identify unauthorized software execution and alert appropriate personnel for further review.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for identifying authorized software programs. The customer control implementation statement should address the software programs (e.g., whitelisted software) authorized to execute on customer-deployed resources. |
| Part b | **Microsoft Azure (PaaS)**  Microsoft Azure implements portions of configuration management controls for operating systems leveraged by PaaS customers.  Microsoft Azure employs a deny-by-default, permit-by-exception software policy. Any changes to baselines or configuration scripts must be reviewed and approved by the appropriate CAB.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for employing a deny-all, permit-by-exception policy to allow the execution of authorized software programs on customer-deployed resources. The customer control implementation statement should address the employed policy. |
| Part c | **Microsoft Azure (PaaS)**  Microsoft Azure implements portions of configuration management controls for operating systems leveraged by PaaS customers.  Microsoft Azure service teams review and update baselines and configuration scripts at least annually.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for reviewing and updating the list of authorized software programs. The customer control implementation statement should address the frequency with which the authorized software list is reviewed and updated. |

### 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: *<Customer-defined>*;Microsoft Azure | |
| Parameter CM-8(a)(4): *<Customer-defined information deemed necessary to achieve effective information system components accountability>* | |
| Parameter CM-8(b): *<FedRAMP Assignment: 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CM-8 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (PaaS)**  Microsoft Azure implements portions of configuration management controls for operating systems leveraged by PaaS customers. Microsoft Azure collects inventory information for the following components:   * Physical devices * Native OS * Guest OS * Web endpoints   After collecting inventory information, Microsoft Azure performs month-over-month data analysis and reconciliation. Any changes to, additions to, or removals from the inventory are identified, verified, and explained.  Microsoft Azure collects, at minimum, the following information for each asset in the inventory:   * Unique asset identifier * NetBIOS name * Baseline configuration name * OS Name * OS Version * Service team   **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for developing and documenting an inventory of customer-deployed resources. The customer control implementation statement should address the process to ensure that the inventory accurate reflects the current system, includes all customer-deployed resources, is granular enough to support tracking and reporting, and includes any information the customer has deemed necessary to achieve effective accountability. |
| Part b | **Microsoft Azure (PaaS)**  Microsoft Azure implements portions of configuration management controls for operating systems leveraged by PaaS customers.  Microsoft Azure updates the system inventory at least monthly, and includes updated inventory information in the monthly Continuous Monitoring report provided to the FedRAMP JAB.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for reviewing and updating the inventory defined in CM-08.a. The customer control implementation statement should address the frequency with which the inventory is reviewed and updated. |

#### 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.

Instruction: A description of the inventory information is documented in Section 10. It is not necessary to re-document it here.

Delete this and all other instructions from your final version of this document.

| CM-8 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>*;Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CM-8 (1) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (PaaS)**  Microsoft Azure implements portions of configuration management controls for operating systems leveraged by PaaS customers.  Microsoft Azure updates the inventory as an integral part of component installations, removals, and information system updated by updating the asset management tool each time a server or network device is included or removed from the production environment. Additionally, Microsoft Azure generates a complete inventory each month, and analyzes and reconciles all changes from the previous month’s inventory.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for reviewing and updating the inventory of customer-deployed resources when required. The customer control implementation statement should address how the inventory is reviewed and updated when installations, removals, and system updates occur. |

#### CM-8 (2) Control Enhancement (H)

The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components.

| CM-8 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CM-8 (2) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for employing automated mechanisms to maintain the inventory of customer-deployed resources. The customer control implementation statement should address the mechanisms used to maintain an up-to-date, complete, accurate, and readily available inventory. |

#### 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: *<Customer-defined>*;Microsoft Azure | |
| Parameter CM-8(3)(a): *<FedRAMP Assignment: continuously, using automated mechanisms with a maximum five-minute delay in detection>* | |
| Parameter CM-8(3)(b): *<FedRAMP Assignment: selection (one or more): disables network access by such components; isolates the components; notifies organization-defined personnel or roles>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CM-8 (3) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (PaaS)**  Microsoft Azure implements portions of configuration management controls for operating systems leveraged by PaaS customers.  Virtual components within Microsoft Azure are managed by the Fabric Controller (FC), which is the component that is used to create, monitor, restart, and destroy virtual machines. The FC monitors the virtual environment, and detects if there are any unauthorized virtual machines that have been deployed.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for employing automated mechanisms to detect the presence of unauthorized software within customer-deployed resources. The customer control implementation statement should address the mechanisms in place to detect unauthorized software and the frequency with which these mechanisms will be employed. |
| Part b | **Microsoft Azure (PaaS)**  Microsoft Azure implements portions of configuration management controls for operating systems leveraged by PaaS customers.  Microsoft Azure does not wait to disable network access for unauthorized components/devices into the information system. When network devices are deployed, ports are turned off by default. Unassigned ports are put into a VLAN that is not configured at the Layer 3 (L3) and has no provisioned servers in it, so even if ports were enabled, there would be no access to any provisioned servers and should not have the ability to leave the subnet. To prevent IP spoofing, Microsoft Azure uses ACLs on the L3 to deny packets sourced by the subnet from entering that subnet.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for taking action when unauthorized software is detected. The customer control implementation statement should address the selected action(s) to be taken (e.g., notifying personnel, isolating resources, and disabling network access), as well as the personnel/roles to be notified (if applicable). |

#### CM-8 (4) Control Enhancement (H)

The organization includes in the information system component inventory information, a means for identifying by [Selection (one or more): name; [FedRAMP Assignment: position and role]], individuals responsible/accountable for administering those components.

| CM-8 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter CM-8 (4): *<FedRAMP Assignment: position and 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CM-8 (4) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for including the individual(s) responsible/accountable for administering the customer-deployed resources listed in the inventory (see CM-08.a). The customer control implementation statement should address the means for identifying (e.g., name, position, or role) the responsible/accountable individuals. |

#### 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-8 (5) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>*;Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CM-8 (5) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (PaaS)**  Microsoft Azure implements portions of configuration management controls for operating systems leveraged by PaaS customers.  Native and Guest OS assets information includes the responsible Azure service team. This ensures that no other information system will identify a Native or Guest OS asset as part of that information system. Service teams own and manage Microsoft Azure subscriptions which they use to deploy virtual machines and other services. Each subscription has a corresponding subscription ID; subscription IDs are unique, and are not shared by multiple service teams.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for verifying that resources are not included in multiple system inventories. The customer control implementation statement should address how the customer verifies that all customer-deployed resources within the authorization boundary are not duplicated in other resource inventories. |

### 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: *<Customer-defined>*;Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CM-9 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (PaaS)**  Microsoft Azure implements portions of configuration management controls for operating systems leveraged by PaaS customers.  Microsoft Azure has a system-wide configuration management plan titled Microsoft Azure Configuration Management Plan. This document contains high level roles and responsibilities, defines configuration management processes, and identifies configuration items as well as processes for maintaining configuration items. Each service team complies with this configuration management plan. The plan is reviewed at least annually and is maintained by Azure Compliance.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for developing, documenting, and implementing a configuration management plan for customer-deployed resources. The customer control implementation statement should address how the configuration management plan addresses roles, responsibilities, and configuration management processes and procedures. |
| Part b | **Microsoft Azure (PaaS)**  Microsoft Azure implements portions of configuration management controls for operating systems leveraged by PaaS customers.  Changes released to the environment are tracked via change management systems for Microsoft Azure either via TFS or the Release to Operations (RTO) tool. Both tools require that the service team has defined their release types with release criteria, including approvals.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for developing, documenting, and implementing a configuration management plan for customer-deployed resources. The customer control implementation statement should address how the configuration management plan establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items. |
| Part c | **Microsoft Azure (PaaS)**  Microsoft Azure implements portions of configuration management controls for operating systems leveraged by PaaS customers.  Microsoft Azure defines the configuration management items for the information system. Microsoft Azure is aligned with the Microsoft’s SDL process which documents each phase of the development life cycle that is followed for all engineering and development projects. The SDL covers the change management process around information system design, development and implementation of changes. In addition, Microsoft Azure is assigned MSEC Advisory who reviews and approves major releases which impact Microsoft Azure environment.  Microsoft Azure software development is aligned with the SDL, and all provisioned hardware and network infrastructure is managed by the Microsoft Azure Operations and Component teams.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for developing, documenting, and implementing a configuration management plan for customer-deployed resources. The customer control implementation statement should address how the configuration management plan defines the configuration items for the customer-deployed resources and places the configuration items under configuration management. |
| Part d | **Microsoft Azure (PaaS)**  Microsoft Azure implements portions of configuration management controls for operating systems leveraged by PaaS customers.  The Microsoft Azure Configuration Management Plan document is stored within the Microsoft Azure SharePoint site, which has functionality to protect against unauthorized disclosure and modification.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for developing, documenting, and implementing a configuration management plan for customer-deployed resources. The customer control implementation statement should address how the configuration management plan protects the configuration management plan from 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: *<Customer-defined>*;Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CM-10 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (PaaS)**  Microsoft Azure implements portions of configuration management controls for operating systems leveraged by PaaS customers.  The Microsoft Online Services Acceptable Use Policy (available for 3PAO review onsite) 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.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for using software and associated documentation in accordance with contract agreements and copyright laws. The customer control implementation statement should address the software in use, as well as the relevant contracts/agreements and copyright laws. |
| Part b | **Microsoft Azure (PaaS)**  Microsoft Azure implements portions of configuration management controls for operating systems leveraged by PaaS customers.  The Microsoft Azure Security Policy outlines the software usage restrictions for Microsoft Azure and requires all Microsoft Azure applications, including those developed or hosted by and/or purchased from third parties, to undergo a comprehensive security review before entry into the Microsoft Azure environment. In addition, no software is to be deployed or used in Microsoft Azure’s production environment without formal approval as required by the Microsoft Azure Security Policy.  In-house software used within the Microsoft Azure boundary is developed by Microsoft and, therefore, not subject to contractual requirements, copyright restrictions, and licenses monitoring for compliance with third-party relationships. In regards to third-party relationships, Microsoft complies with all software usage requirements as defined by the contractual agreement with the vendor.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for tracking the use of software and associated documentation protected by quantity licenses. The customer control implementation statement should address how software usage is tracked to control copying and distribution. |
| Part c | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for controlling and documenting of the use of peer-to-peer (P2P) file sharing technology. The customer control implementation statement should address how the customer controls and documents the use of P2P file sharing to prevent unauthorized distribution, display, performance, or reproduction of copyrighted work. |

#### 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: *<Customer-defined>*;Microsoft Azure | |
| Parameter CM-10(1): *<Customer-defined restrictions>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CM-10 (1) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (PaaS)**  Microsoft Azure implements portions of configuration management controls for operating systems leveraged by PaaS customers.  As established by the Microsoft Azure Security Policy, the following restrictions are in place regarding the installation of software, including open source software, within the Microsoft Azure environment: All software (including tools and utilities) installed within Microsoft Azure must be approved by the appropriate stakeholders prior to being released into production.  Prior to deployment in Microsoft Azure, all software must be tested in a manner suitable to Microsoft to evaluate its impact on system performance, stability (failure and recovery characteristics) and security state (security controls work as expected and the product does not contain malicious code).  Software submitted for approval must have a legitimate business purpose.  Additionally, open source software must be evaluated by LCA in accordance with guidance provided within the LCA SharePoint. Requests for evaluation of open source software require approval through the LCA OSS Approval Tool.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for restricting the use of open source software. The customer control implementation statement should address the customer-defined restrictions that govern the use of open source software. |

### 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: *<Customer-defined>*;Microsoft Azure | |
| Parameter CM-11(a): *<Customer-defined policies>* | |
| Parameter CM-11(b): *<Customer-defined methods>* | |
| Parameter CM-11(c): *<FedRAMP Assignment: continuously (via CM-7 (5))>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CM-11 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (PaaS)**  Microsoft Azure implements portions of configuration management controls for operating systems leveraged by PaaS customers.  As established by the Microsoft Azure Security Policy, the following restrictions are in place regarding the installation of software, including open source software, within the Microsoft Azure environment:  All software (including tools and utilities) installed within Microsoft Azure must be approved by the appropriate stakeholders prior to being released into production.  Prior to deployment in Microsoft Azure, all software must be tested in a manner suitable to Microsoft to evaluate its impact on system performance, stability (failure and recovery characteristics) and security state (security controls work as expected and the product does not contain malicious code).  Software submitted for approval must have a legitimate business purpose.  Additionally, open source software must be evaluated by LCA in accordance with guidance provided within the LCA SharePoint. Requests for evaluation of open source software require approval through the LCA OSS Approval Tool.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for restricting the use of open source software. The customer control implementation statement should address the customer-defined restrictions that govern the use of open source software. |
| Part b | **Microsoft Azure (PaaS)**  Microsoft Azure implements portions of configuration management controls for operating systems leveraged by PaaS customers.  Microsoft Azure enforces software installation policies through configuration control processes described in CM-3 and access restrictions for change described in CM-5.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for enforcing software installation policies. The customer control implementation statement should address the customer-defined methods through which software installation policies are enforced. |
| Part c | **Microsoft Azure (PaaS)**  Microsoft Azure monitors compliance as described in CM-7(5).  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for monitoring the compliance of customer-deployed resources with the policies identified in CM-11.a. The customer control implementation statement should address the frequency at which policy compliance is monitored. |

#### CM-11 (1) Control Enhancement (H)

The information system alerts [Assignment: organization-defined personnel or roles] when the unauthorized installation of software is detected.

| CM-11 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter CM-11 (1): *<Customer-defined personnel or roles>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CM-11 (1) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for providing alerts when the unauthorized installation of software is detected. The customer control implementation statement should address the personnel/roles to be alerted. |

## Contingency Planning (CP)

### CP-1 Contingency Planning Policy and Procedures (H)

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 annually].; and
   2. Contingency planning procedures [FedRAMP Assignment: at least annually or whenever a significant change occurs].

| CP-1 | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter CP-1(a): *<Customer-defined personnel or roles>* | |
| Parameter CP-1(b)(1): *<FedRAMP Assignment: at least annually>* | |
| Parameter CP-1(b)(2): *<FedRAMP Assignment: at least annually or whenever a significant change occurs>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| CP-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for developing, documenting, reviewing, updating, and disseminating contingency planning policy and procedures for customer-deployed resources. The customer control implementation statement should address the content of the policy (which must include purpose, scope, roles, responsibilities, management commitment, coordination, and compliance), procedures (which must facilitate the implementation of the policies and associated controls), the frequency of review, and the role(s) responsible. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for developing, documenting, reviewing, updating, and disseminating contingency planning policy and procedures for customer-deployed resources. The customer control implementation statement should address the content of the policy (which must include purpose, scope, roles, responsibilities, management commitment, coordination, and compliance), procedures (which must facilitate the implementation of the policies and associated controls), the frequency of review, and the role(s) responsible. |

### CP-2 Contingency Plan (L) (M) (H)

The organization:

1. Develops a contingency plan for the information system that:

Identifies essential missions and business functions and associated contingency requirements;

Provides recovery objectives, restoration priorities, and metrics;

Addresses contingency roles, responsibilities, assigned individuals with contact information;

Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;

Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and

Is reviewed and approved by [Assignment: organization-defined personnel or roles];

Distributes copies of the contingency plan to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements];

Coordinates contingency planning activities with incident handling activities;

Reviews the contingency plan for the information system [FedRAMP Assignment: at least annually];

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;

Communicates contingency plan changes to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]; and

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: *<Customer-defined>* | |
| Parameter CP-2(a)(6): *<Customer-defined personnel or roles>* | |
| Parameter CP-2(b): *<Customer-defined key contingency personnel (identified by name and/or by role) and organizational elements>* | |
| Parameter CP-2(d): *<FedRAMP Assignment: at least annually>* | |
| Parameter CP-2(f): *<Customer-defined key contingency personnel (identified by name and/or by role) and organizational elements>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CP-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for developing a contingency plan for customer-deployed resources. The customer control implementation statement should address the essential mission and business functions and associated contingency requirements; recovery objectives, restoration priorities and metrics; contact information for assigned roles/responsibilities/individuals; maintaining essential mission and business functions despite system disruption, compromise or failure; eventual, full system restoration without deterioration of originally implemented security safeguards; and review/approval of the plan by customer-defined personnel/roles. Note: the customer should also include any reliance on Microsoft Azure functionality to perform these tasks. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for distributing the contingency plan. The customer control implementation statement should address the key personnel (identified by name and/or role) and customer elements who should receive a copy of the contingency plan defined in CP-02.a. |
| Part c | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for coordinating contingency planning with incident handling. The customer control implementation statement should address the process in which planned contingency activities are coordinated with incident handling activities. |
| Part d | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for reviewing the contingency plan. The customer control implementation statement should address the frequency with which the contingency plan is reviewed. |
| Part e | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for updating the contingency plan. The customer control implementation statement should address how updates reflect changes to the organization, resources, or environment of operation; and the problems encountered during implementation, execution, or testing of contingency activities. |
| Part f | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for communicating changes made to the contingency plan. The customer control implementation statement should address the means by which the customer communicates changes to the key personnel defined in CP-02.b. |
| Part g | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for protecting the contingency plan. The customer control implementation statement should address the process for preventing unauthorized disclosure or modification of the plan. |

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

The organization coordinates contingency plan development with organizational elements responsible for related plans.

| CP-2 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CP-2 (1) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for coordinating contingency plan development with organizational elements responsible for related plans (e.g., business continuity, disaster recovery). The customer control implementation statement should address the coordination of initial plan development, as well as how updates to the contingency plan affect related plans and vice versa. |

#### 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-2 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>*; Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CP-2 (2) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure has implemented a capacity planning process that ensures adequate resources are available for the Microsoft Azure environment. The capacity management process includes the determination of the overall size, performance and resilience of the system. The capacity management process includes the following activities:   * Understanding the current demands and forecasting the future requirements * Monitoring performance and throughput of services and supporting infrastructure components * Carry out tuning activities to ensure efficient utilization of available resources * Establishing and enforcing the policy for platform services contingency capacity buffer   **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for conducting capacity planning to ensure customer-deployed resources continue operating during contingency activities. The customer control implementation statement should address how the necessary capacity is available for processing, telecommunications, and environmental support during contingency operations. Note: if the customer configures Microsoft Azure appropriately for reserving processing capacity in an alternate region, Azure can support continued system operation during contingency activities. |

#### 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-2 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>*; Microsoft Azure | |
| Parameter CP-2(3): *<Customer-defined time period>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CP-2 (3) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure establishes recovery time objectives (RTO) for essential Microsoft Azure missions and business functions and documents those objectives as part of the BCM process.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for resuming essential mission and business functions once contingency activities have commenced. The customer control implementation statement should address the time period within which essential mission and business functions must resume after contingency plan activation. Note: if the customer configures Microsoft Azure appropriately for reserving processing capacity in an alternate region, Azure can support continued system operation during contingency activities. |

#### CP-2 (4) Control Enhancement (H)

The organization plans for the resumption of all missions and business functions within [FedRAMP Assignment: time period defined in service provider and organization Service Level Agreement (SLA)] of contingency plan activation.

| CP-2 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>*; Microsoft Azure | |
| Parameter CP-2 (4): *<FedRAMP Assignment: time period defined in service provider and organization Service Level Agreement (SLA)>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CP-2 (4) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure establishes recovery time objectives (RTO) for all Microsoft Azure missions and business functions and documents those objectives as part of the BCM process.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for resuming all mission and business functions once contingency activities have commenced. The customer control implementation statement should address the time period within which all mission and business functions must resume after contingency plan activation. Note: if the customer configures Microsoft Azure appropriately for reserving processing capacity in an alternate region, Azure can support continued system operation during contingency activities. |

#### CP-2 (5) Control Enhancement (H)

The organization plans for the continuance of essential missions and business functions with little or no loss of operational continuity and sustains that continuity until full information system restoration at primary processing and/or storage sites.

| CP-2 (5) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>*; Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CP-2 (5) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure has planned for the continuance of essential missions and business functions by establishing alternate storage and processing sites at geographically distributed Azure data centers. Data is replicated between primary and alternate sites. Alternate sites have physical and logical security safeguards equivalent to primary sites.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for continuing essential mission and business functions until customer-deployed resources have been restored at primary sites. The customer control implementation statement should address how the customer continues essential mission and business functions with little or no loss of operational continuity and sustains that continuity until full resource restoration has occurred at primary processing and/or storage sites. Note: if the customer configures Microsoft Azure appropriately for reserving processing capacity in an alternate region, Azure can support continued system operation during contingency activities. |

#### CP-2 (8) Control Enhancement (M) (H)

The organization identifies critical information system assets supporting essential missions and business functions.

| CP-2 (8) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CP-2 (8) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for identifying critical customer-deployed resources. The customer control implementation statement should address any resources that support essential mission and business functions during contingency operations. |

### 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;

When required by information system changes; and

[FedRAMP Assignment: at least annually] thereafter.

| CP-3 | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter CP-3(a): *<FedRAMP Assignment: ten (10) days>* | |
| Parameter CP-3(c): *<FedRAMP Assignment: 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CP-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for providing contingency training to users of customer-deployed resources in accordance with assigned roles and responsibilities. The customer control implementation statement should address the time period within which personnel assuming a contingency role/responsibility must be trained. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for providing contingency retraining to users of customer-deployed resources, when changes occur, in accordance with assigned roles and responsibilities. The customer control implementation statement should address the types of changes to customer-deployed resources that necessitate retraining. |
| Part c | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for providing contingency retraining to users of customer-deployed resources, as required, in accordance with assigned roles and responsibilities. The customer control implementation statement should address the customer-defined frequency with which retraining is required. |

#### CP-3 (1) Control Enhancement (H)

The organization incorporates simulated events into contingency training to facilitate effective response by personnel in crisis situations.

| CP-3 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CP-3 (1) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for facilitating effective response by personnel in crisis situations. The customer control implementation statement should address the incorporation of simulated events into contingency training. |

### 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.

Reviews the contingency plan test results; and

Initiates corrective actions, if needed.

| CP-4 | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter CP-4(a)-1: *<FedRAMP Assignment: at least annually>* | |
| Parameter CP-4(a)-2: *<FedRAMP Assignment: 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CP-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for testing the contingency plan for customer-deployed resources. The customer control implementation statement should address the frequency and tests performed to determine the effectiveness of the contingency plan and the organizational readiness to execute the plan. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for reviewing the results of contingency plan testing (see CP-04.a). The customer control implementation statement should address the process of reviewing contingency plan test results. |
| Part c | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for initiating corrective action regarding contingency plan testing. The customer control implementation statement should address any corrective actions taken upon review of contingency plan test results (see CP-04.b). |

#### CP-4 (1) Control Enhancement (M) (H)

The organization coordinates contingency plan testing and/or exercises with organizational elements responsible for related plans.

| CP-4 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CP-4 (1) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for coordinating contingency plan testing with the testing of related plans. The customer control implementation statement should address the coordination of contingency plan testing with organizational elements responsible for related plans (e.g., business continuity, disaster recovery). |

#### CP-4 (2) Control Enhancement (H)

The organization tests the contingency plan at the alternate processing site:

1. To familiarize contingency personnel with the facility and available resources; and
2. To evaluate the capabilities of the alternate processing site to support contingency operations.

| CP-4 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>*; Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CP-4 (2) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure performs alternate site testing as part of continuity planning. This type of exercise requires personnel responsible for recovery to engage individuals responsible for Data Center recovery, and to coordinate contingency plan testing and/or exercises with other Azure service teams as deemed necessary for the simulated recovery of all related plans and ensure adequate resources are available for Microsoft Azure.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for testing the contingency plan at an alternate processing location. The customer control implementation statement should address how testing familiarizes contingency personnel with the facility and resources available at the alternate site. Note: if the customer configures Microsoft Azure appropriately for reserving processing capacity in an alternate region, Azure can support contingency testing and provide continued system operation during contingency activities. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure performs failover testing to verify that alternate processing sites are able to support contingency operations.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for testing the contingency plan at an alternate processing location. The customer control implementation statement should address the evaluation of the alternate processing site and its capability to support contingency operations. Note: if the customer configures Microsoft Azure appropriately for reserving processing capacity in an alternate region, Azure can support contingency testing and provide continued system operation during contingency activities. |

### 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: *<Customer-defined>*; Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CP-6 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure establishes alternate storage sites at geographically distributed Microsoft datacenters. Data durability is obtained by synchronously replicating data across different databases in the same datacenter and across multiple datacenters. Disaster Recovery is achieved by asynchronous replication to a DC in a different geographical region.  High-level customer configuration data is automatically replicated across geo-replicated DCs (across DBs in active datacenters) in real time. All in-scope data is backed up and stored in a geographically separate location and the ability to revert to an alternative instance is validated on a quarterly basis.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for establishing an alternate storage site. The customer control implementation statement should address the customer's ability to store and retrieve backup information, and the agreements permitting such activities. Note: if the customer configures Microsoft Azure appropriately for reserving storage capacity in an alternate region, Azure can support the secure storage and retrieval of system data. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure alternate storage sites have physical and logical security safeguards equivalent to that of the primary site.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for establishing an alternate storage site. The customer control implementation statement should address how the security safeguards of the alternate storage site are equivalent to that of the primary site. Note: if the customer configures Microsoft Azure appropriately for reserving storage capacity in an alternate region, Azure can support the secure storage and retrieval of system data. |

#### 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-6 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>*; Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CP-6 (1) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure has identified and deployed multiple primary and secondary storage sites that are geographically separated so as not to be susceptible to the same hazards.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for establishing an alternate storage site. The customer control implementation statement should address how the alternate storage site is separated from the primary storage site to reduce its susceptibility to the same threats (e.g., natural disasters). Note: if the customer configures Microsoft Azure appropriately for reserving storage capacity in an alternate region, Azure can support the secure storage and retrieval of system data. |

#### CP-6 (2) Control Enhancement (H)

The organization configures the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives.

| CP-6 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>*; Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CP-6 (2) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure leverages a Hot/Hot architecture that allows alternative site storage to be continuously available.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for establishing an alternate storage site. The customer control implementation statement should address how the alternate storage site facilitates recovery operations consistent with customer-defined recovery time objectives (RTO's) and recovery point objectives (RPO's). Note: if the customer configures Microsoft Azure appropriately for reserving storage capacity in an alternate region, Azure can support the secure storage and retrieval of system data. |

#### 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-6 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CP-6 (3) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure manages all Microsoft datacenters and has Emergency Management Teams (EMT) in place to discuss with all team members any accessibility problems to alternate processing sites in the event of an area-wide disruption or disaster and details explicit mitigation actions. If there is a disruption to the primary site, Azure personnel from that site do not have to go to the secondary site, as there are Azure personnel already engaged and operating in the secondary site. An area-wide disruption or disaster at the primary site would not affect the Microsoft Azure secondary storage site since they are located in geographically separated regions for each system.  Microsoft Azure personnel with logical access are located in Puget Sound, working remotely; therefore, there are no accessibility concerns for logical administration of Microsoft Azure.  **Customer Responsibility (IaaS/PaaS)**  Customers do not have access to manage accessibility to system resources in Azure datacenters; alternative site accessibility controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure. |

### 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.

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

Ensures that the alternate processing site provides information security safeguards equivalent to that of the primary site.

| CP-7 | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>*; Microsoft Azure | |
| Parameter CP-7(a)-1: *<Customer-defined information system operations>* | |
| Parameter CP-7(a)-2: *<FedRAMP Assignment: The service provider defines a time period consistent with the recovery time objectives and business impact analysis>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CP-7 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  Microsoft datacenters used for Microsoft Azure are owned and managed by Microsoft. Microsoft Azure has established multiple alternate processing sites (identically replicated and backed up) which allow the resumption of information system operations for essential missions and business functions when the primary processing site cannot be restored. Microsoft Azure backup and recovery procedures around data replication using the four methods described in control CP-6, along with geo-replication, allow operations to resume within the time period defined in the Microsoft Azure Contingency Plan.  Microsoft Azure has identified the primary and secondary alternative processing sites discussed in CP-6 (1) that are geographically separated so as not to be susceptible to the same hazards as documented in CP-6.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for establishing an alternate processing site. The customer control implementation statement should address the agreements permitting the transfer and resumption of customer-defined system operations consistent with customer-defined recovery time and recovery point objectives when the primary processing site is unavailable. Note: if the customer configures Microsoft Azure appropriately for reserving processing capacity in an alternate region, Azure can support the continuation of secure system operation. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  Microsoft takes an infrastructure approach to disaster recovery, providing the capabilities required for customers to implement the recovery appropriate for their business. Customers must follow the appropriate guidance to ensure correct implementation of their business continuity solution. For example, to protect Azure Storage data from a region wide disaster storage accounts must be configured to use geo-replication (GRS or RA-GRS).  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for establishing an alternate processing site. The customer control implementation statement should address the resources available at the alternate processing site and their ability to transfer and resume operations within the time period defined in CP-07.a. Note: if the customer configures Microsoft Azure appropriately for reserving processing capacity in an alternate region, Azure can support the continuation of secure system operation. |
| Part c | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure alternate processing sites have physical and logical security safeguards equivalent to that of the primary site.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for establishing an alternate processing site. The customer control implementation statement should address how the security safeguards of the alternate processing site are equivalent to that of the primary site. Note: if the customer configures Microsoft Azure appropriately for reserving processing capacity in an alternate region, Azure can support the continuation of secure system operation. |

#### 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-7 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>*; Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CP-7 (1) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure has established multiple alternate processing sites that are separated from the primary processing site so as not to be susceptible to the same physical hazards.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for establishing an alternate processing site. The customer control implementation statement should address how the alternate site is separated from the primary processing site to reduce its susceptibility to the same threats (e.g., natural disasters). Note: if the customer configures Microsoft Azure appropriately for reserving processing capacity in an alternate region, Azure can support the continuation of secure system operation. |

#### 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-7 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CP-7 (2) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure manages all Microsoft datacenters and has Emergency Management Teams (EMT) in place to discuss with all team members any accessibility problems to alternate processing sites in the event of an area-wide disruption or disaster and details explicit mitigation actions. If there is a disruption to the primary site, Azure personnel from that site do not have to go to the secondary site, as there are Azure personnel already engaged and operating in the secondary site. An area-wide disruption or disaster at the primary site would not affect the Microsoft Azure secondary storage site since they are located in geographically separated regions for each system.  Microsoft Azure personnel with logical access are located in Puget Sound, working remotely; therefore, there are no accessibility concerns for logical administration of Microsoft Azure.  **Customer Responsibility (IaaS/PaaS)**  Customers do not have access to manage accessibility to system resources in Azure datacenters; alternative site accessibility controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure. |

#### 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-7 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>*; Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CP-7 (3) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure's primary and alternate processing sites are located within Microsoft datacenters. Therefore, it is not necessary for site agreements to be in place. Priority-of-service provisions are not required because Microsoft owns and manages all of the datacenter facilities.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for establishing an alternate processing site. The customer control implementation statement should address the agreements containing priority-of-service provisions which correspond with customer-defined availability requirements (e.g., RTO's). Note: if the customer configures Microsoft Azure appropriately for reserving processing capacity in an alternate region, Azure can support the continuation of secure system operation. |

#### CP-7 (4) Control Enhancement (H)

The organization prepares the alternate processing site so that the site is ready to be used as the operational site supporting essential missions and business functions.

| CP-7 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>*; Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CP-7 (4) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure deploys its various alternative sites in active-active configurations and these sites are always ready to be used as operational sites supporting all missions and business functions.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for establishing an alternate processing site. The customer control implementation statement should address the preparation of the alternate site for use as the operational site supporting essential missions and business functions. Note: if the customer configures Microsoft Azure appropriately for reserving processing capacity in an alternate region, Azure can support the continuation of secure system operation. |

### 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-8 | Control Summary Information |
| --- | --- |
| Responsible Role: Microsoft Azure | |
| Parameter CP-8-1: All information system operations | |
| Parameter CP-8-2: Recovery time objectives identified in Microsoft Azure BCPs | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CP-8 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure is located within Microsoft Azure datacenters. Microsoft Azure is responsible for ensuring continuity of its telecommunications services through the process of utilizing diverse fiber routes and redundant hardware to provide maximum availability. Each of the datacenters represented as part of the Microsoft Azure boundary are active, independent from each other, and fully operational with the ability to provide services at any time. In addition to the active datacenter configuration, Microsoft Azure additionally mitigates the risk of single points of failures with telecommunication links by requiring each datacenter to have at least two diverse fiber paths. Microsoft owns and maintains its own fiber network whose purpose is to exclusively support Microsoft properties, acting as a global fiber backbone comparable to multiple ISPs. Microsoft contracts with Level 3 Communications to provide field service maintenance in the event of faults, defects, or failures. The service level objective for on-demand maintenance and critical time to repair is 4 hours. Critical problems are defined as incidents or outages, other than caused by an Excused Outage, which cause a Microsoft Equipment failure, as a result of which Microsoft cannot receive any data.  **Customer Responsibility (IaaS/PaaS)**  Customers are not responsible for datacenter operations (to include telecommunications services). All telecommunication services are provided and managed by Microsoft Azure. This control is inherited from Azure. |

#### 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: Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CP-8 (1) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure is located within Microsoft Azure datacenters. Microsoft Azure controls its own network routing, and therefore, Service Priority setting for emergency purposes is not required. Microsoft Azure is responsible for defining its own routing priority based on property availability requirements and emergency purposes. In the cloud environment, there is no priority order because there are different teams to bring each specific component back online in the RTOs defined for each component. All components are therefore a priority in an outage scenario.  **Customer Responsibility (IaaS/PaaS)**  Customers are not responsible for datacenter operations (to include telecommunications services). All telecommunication services are provided and managed by Microsoft Azure. This control is inherited from Azure. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure is located within Microsoft Azure datacenters. Microsoft Azure controls its own network routing, and therefore, Service Priority setting for emergency purposes is not required.  **Customer Responsibility (IaaS/PaaS)**  Customers are not responsible for datacenter operations (to include telecommunications services). All telecommunication services are provided and managed by Microsoft Azure. This control is inherited from Azure. |

#### 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-8 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CP-8 (2) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure mitigates the risk of single points of failures with telecommunication links by requiring each datacenter to have at least two diverse fiber paths. Microsoft owns and maintains its own fiber network whose purpose is to exclusively support Microsoft properties, acting as a global fiber backbone comparable to multiple ISPs. Microsoft Azure contracts with a large provider to provide field service maintenance in the event of faults, defects, or failures. The service level objective for on-demand maintenance and critical time to repair is 4 hours.  **Customer Responsibility (IaaS/PaaS)**  Customers are not responsible for datacenter operations (to include telecommunications services). All telecommunication services are provided and managed by Microsoft Azure. This control is inherited from Azure. |

#### CP-8 (3) Control Enhancement (H)

The organization obtains alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats.

| CP-8 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CP-8 (3) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure mitigates the risk of single points of failures with telecommunication links by requiring each Azure data center to have at least two diverse fiber paths. The redundant communication links were established following disparate paths through the Microsoft fiber network. This is a continuously operational solution managed by Azure.  **Customer Responsibility (IaaS/PaaS)**  Customers are not responsible for datacenter operations (to include telecommunications services). All telecommunication services are provided and managed by Microsoft Azure. This control is inherited from Azure. |

#### CP-8 (4) Control Enhancement (H)

The organization:

1. Requires primary and alternate telecommunications service providers to have contingency plans;

Reviews provider contingency plans to ensure that the plans meet organizational contingency requirements; and

Obtains evidence of contingency testing/training by providers [FedRAMP Assignment: annually].

| CP-8 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: Microsoft Azure | |
| Parameter CP-8 (4)(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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CP-8 (4) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure has implemented the contingency planning policy through the publication of the Microsoft Security Policy, maintained by Azure security. The Azure continuity management policy objective is to protect external customers and the internal Microsoft business by providing a service and functional resiliency along with a recovery capability to restore the subscribed services and business core competencies in a predetermined timeframe during a significant outage.  **Customer Responsibility (IaaS/PaaS)**  Customers are not responsible for datacenter operations (to include telecommunications services). All telecommunication services are provided and managed by Microsoft Azure. This control is inherited from Azure. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure’s Security Policy is reviewed and approved annually by Azure Security Management and maintained in the GRC tool. The Microsoft Security Policy applies across the organization 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.  **Customer Responsibility (IaaS/PaaS)**  Customers are not responsible for datacenter operations (to include telecommunications services). All telecommunication services are provided and managed by Microsoft Azure. This control is inherited from Azure. |
| Part c | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure implements contingency plan testing and exercises by following the policy set forth in the Azure Datacenter ERDRP. Contingency plan testing and maintenance procedures are implemented with the goal of maintaining the ERDRP in a consistent state of readiness. These procedures apply to the continued maintenance, testing, and training requirements of the ERDRP. The coordination of the ERDRP is the responsibility of the Datacenter Manager. The Datacenter Manager is responsible for the review and testing of the ERDRP at least annually.  **Customer Responsibility (IaaS/PaaS)**  Customers are not responsible for datacenter operations (to include telecommunications services). All telecommunication services are provided and managed by Microsoft Azure. This control is inherited from Azure. |

### 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: *<Customer-defined>*; Microsoft Azure | |
| Parameter CP-9(a): <*FedRAMP Assignment: daily incremental; weekly full>* | |
| Parameter CP-9(b): *<FedRAMP Assignment: daily incremental; weekly full>* | |
| Parameter CP-9(c): *<FedRAMP Assignment: daily incremental; weekly full>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CP-9 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure synchronously replicates user level information stored in Azure storage. This data is synchronously replicated locally using the EC14+4 algorithm which provides redundancy equivalent to three copies. In addition, data is asynchronously replicated to a remote region for accounts which have configured GRS or RA-GRS.  For user level information stored in Microsoft Azure SQL DB, data is replicated synchronously across three SQL DB storage nodes within a region. automatically copies the backups of customer data to the storage site within the same datacenter. This data is also automatically geo-replicated to the alternative storage site in a different geographic region. If the datacenter hosting the customer data fails, the customers can utilize the Microsoft Azure Management Portal or programmatic API to restore their data from the geo-replicated backup to any geographic region of their choice.  **Customer Responsibility (PaaS)**  The customer is responsible for conducting backups for customer-deployed resources (to include applications, databases, and software). The customer control implementation statement should address the frequency (to be consistent with customer-defined RTO's and RPO's) with which user-level information is backed up. Note: if the customer configures Microsoft Azure backup services appropriately, Azure can support data loss prevention.  **Customer Responsibility (IaaS)**  The customer is responsible for conducting backups of customer-deployed resources (to include applications, operating systems, databases, and software). The customer control implementation statement should address the frequency (to be consistent with customer-defined RTO's and RPO's) with which user-level information is backed up. Note: if the customer configures Microsoft Azure backup services appropriately, Azure can support data loss prevention. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure backs up system level information using either Azure Storage continuous replication or SQL Server mirroring. Triple redundancy of backups for Azure Storage is achieved with Erasure Coding described above. Triple redundancy of SQL backups is achieved by maintaining three complete copies of the data. Backup frequency is based on requirements defined by the BIA.  For Microsoft Azure SQL DB, system data (including all configuration files) is backed up to XML. Backups are replicated in DFS (server and database information only, no PII or customer data). The system data backups are accessible via XTS.  At any one time, Microsoft Azure SQL DB keeps three replicas of data running – one primary replica and two secondary replicas. Microsoft Azure SQL DB uses a quorum based commit scheme where data is written to the primary datacenter and one secondary datacenter replica before the transaction is considered committed. If the hardware fails on the primary replica, Microsoft Azure SQL DB detects the failure and fails over to the secondary replica. In case of a physical loss of the replica, Microsoft Azure SQL DB creates a new replica automatically. Therefore, there are at least two physical transaction consistent copies of customer data in the datacenter.  **Customer Responsibility (PaaS)**  The customer is responsible for conducting backups for customer-deployed resources (to include applications, databases, and software). The customer control implementation statement should address the frequency (to be consistent with customer-defined RTO's and RPO's) with which system-level information is backed up. Note: if the customer configures Microsoft Azure backup services appropriately, Azure can support data loss prevention.  **Customer Responsibility (IaaS)**  The customer is responsible for conducting backups of customer-deployed resources (to include applications, operating systems, databases, and software). The customer control implementation statement should address the frequency (to be consistent with customer-defined RTO's and RPO's) with which system-level information is backed up. Note: if the customer configures Microsoft Azure backup services appropriately, Azure can support data loss prevention. |
| Part c | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure stores information system documentation and security-related documentation on Microsoft internal SharePoint sites.  **Customer Responsibility (PaaS)**  The customer is responsible for conducting backups for customer-deployed resources (to include applications, databases, and software). The customer control implementation statement should address the frequency (to be consistent with customer-defined RTO's and RPO's) with which system documentation information is backed up. Note: if the customer configures Microsoft Azure backup services appropriately, Azure can support data loss prevention.  **Customer Responsibility (IaaS)**  The customer is responsible for conducting backups of customer-deployed resources (to include applications, operating systems, databases, and software). The customer control implementation statement should address the frequency (to be consistent with customer-defined RTO's and RPO's) with which system documentation information is backed up. Note: if the customer configures Microsoft Azure backup services appropriately, Azure can support data loss prevention. |
| Part d | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure follows measures to protect the confidentiality/integrity of transmitted information in accordance with FIPS 140-2 by meeting or exceeding requirements as outlined:  Communications between the Microsoft Azure service offerings and the Microsoft Azure Management Portal are configured to require FIPS 140-2 compliant encryption (TLS).  The Microsoft Azure virtual environment enforces key communications between Microsoft Azure internal components to be protected with self-signed SSL certificates.  **Customer Responsibility (PaaS)**  The customer is responsible for protecting backups for customer-deployed resources (to include applications, databases, and software). The customer control implementation statement should address the mechanisms used to protect the confidentiality, integrity, and availability (CIA) of backup data at storage locations. Note: if the customer configures Microsoft Azure backup services appropriately, Azure can support the protection of backup data.  **Customer Responsibility (IaaS)**  The customer is responsible for protecting backups of customer-deployed resources (to include applications, operating systems, databases, and software). The customer control implementation statement should address the mechanisms used to protect the confidentiality, integrity, and availability (CIA) of backup data at storage locations. Note: if the customer configures Microsoft Azure backup services appropriately, Azure can support the protection of backup data. |

#### CP-9 (1) Control Enhancement (H)

The organization tests backup information [FedRAMP Assignment: at least monthly] to verify media reliability and information integrity.

| CP-9 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Microsoft Azure | |
| Parameter CP-9 (1): 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CP-9 (1) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure monitors backups on a continuous basis using system generated alerts which notify Microsoft Azure operations team of any failed or incomplete backups. In addition to system-generated alerts, restoration tests are performed for all backups owned by Microsoft Azure at least every 12 months using the BCDR Manager tool. The integrity of data is automatically confirmed upon completion of the backup.  At any one time, Microsoft Azure SQL DB keeps three replicas of data running – one primary replica and two secondary replicas. Microsoft Azure SQL DB uses a quorum based commit scheme where data is written to the primary and one secondary replica before the transaction is considered committed. If the hardware fails on the primary replica, Microsoft Azure SQL DB detects the failure and fails over to the secondary replica. In case of a physical loss of a replica, Microsoft Azure SQL DB creates a new replica automatically. Therefore, there are at least two physical transaction consistent copies of customer data in the datacenter. Microsoft Azure SQL DB will not write transactions to the database unless primary and secondary replicas are made.  **Customer Responsibility (IaaS/PaaS)**  Microsoft Azure ensures media reliability and information integrity for backups of Azure resources. As such, this control is inherited from Microsoft Azure. |

#### CP-9 (2) Control Enhancement (H)

The organization uses a sample of backup information in the restoration of selected information system functions as part of contingency plan testing.

| CP-9 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>*; Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CP-9 (2) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure does not use any external media for backups. User level information is stored in Azure Storage. Microsoft Azure uses geo-replication to alternate geographic locations. Data durability is obtained by synchronously replicating data across three different databases in different data centers. Restoration tests are performed for all backup data owned by Microsoft Azure at least every 12 months. The restoration tests are captured and stored in the BCDR Manager database in order to generate reports and perform root-cause analysis.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for testing backup information. The customer control implementation statement should address the use of backup information as part of contingency plan testing. Note: if the customer configures Microsoft Azure backup services appropriately, Azure can support the testing of backup information. |

#### 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-9 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>*; Microsoft Azure | |
| Parameter CP-9(3): *<Customer-defined critical information system software and other security-related 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CP-9 (3) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure replicates customer data for customers that have enabled geo-replication. Data is replicated across multiple storage sites that are geographically distributed.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for separately storing backup information. The customer control implementation statement should address the customer-defined critical information to be stored, and the separation of this data from primary customer-deployed resources (e.g., separate facility or fire-rated container that is not collocated). Note: if the customer configures Microsoft Azure backup services appropriately, Azure can support the protection of backup data. |

#### CP-9 (5) Control Enhancement (H)

The organization transfers information system backup information to the alternate storage site [FedRAMP Assignment: time period and transfer rate consistent with the recovery time and recovery point objectives defined in the service provider and organization SLA].

| CP-9 (5) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>*; Microsoft Azure | |
| Parameter CP-9 (5): *<FedRAMP Assignment: time period and transfer rate consistent with the recovery time and recovery point objectives defined in the service provider and organization SLA>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CP-9 (5) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure establishes alternate storage sites at geographically distributed Azure data centers. Data durability is obtained by synchronously replicating data across different databases in the same datacenter and across multiple datacenters. Disaster Recovery is achieved by asynchronous replication to a DC in a different geographical region.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for transferring backup information to an alternate storage site. The customer control implementation statement should address the customer-defined time period and transfer rate (to be consistent with RTO's and RPO's) of backup data to the alternate site. Note: if the customer configures Microsoft Azure backup services appropriately, Azure can support the storage of backup data. |

### 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: *<Customer-defined>*; Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CP-10 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure has developed Business Continuity Plan documents 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 Microsoft Azure system.  **Customer Responsibility (PaaS)**  The customer is responsible for the recovery and reconstitution of customer-deployed resources (to include applications, databases, and software). The customer control implementation statement should address the customer's ability to restore the system after a disruption, compromise, or failure. Note: if the customer configures Microsoft Azure backup and/or alternate site processing services appropriately, Azure can support the continued operation of customer-deployed resources.  **Customer Responsibility (IaaS)**  The customer is responsible for the recovery and reconstitution of customer-deployed resources (to include applications, operating systems, databases, and software). The customer control implementation statement should address the customer's ability to restore the system after a disruption, compromise, or failure. Note: if the customer configures Microsoft Azure backup and/or alternate site processing services appropriately, Azure can support the continued operation of customer-deployed resources. |

#### 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: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CP-10 (2) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for implementing transaction recovery within customer-deployed resources. The customer control implementation statement should address the mechanisms supporting the recovery of resources that are transaction-based (e.g., transaction rollback, transaction journaling). Note: if the customer configures Microsoft Azure backup and/or alternate site processing services appropriately, Azure can support the continued operation of customer-deployed resources. |

#### CP-10 (4) Control Enhancement (H)

The organization provides the capability to restore information system components within [FedRAMP Assignment: time period consistent with the restoration time-periods defined in the service provider and organization SLA] from configuration-controlled and integrity-protected information representing a known, operational state for the components.

| CP-10 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>*; Microsoft Azure | |
| Parameter CP-10 (4): *<FedRAMP Assignment: time period consistent with the restoration time-periods defined in the service provider and organization SLA>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CP-10 (4) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure implements the following process to recover Azure systems in the case that all primary and secondary Data Centers for an Azure system experience failure or if Microsoft were to resume processing at a disrupted site:   * Defined images and current OS (Host OS, Guest OS, Microsoft Azure Virtual Machines, Native OS) and application baselines * Defined security processes around access control, change management, mandatory configuration settings, and encryption mechanisms. Redeployment as part of system restoration follows the same process with the same authentication requirements as initial deployment (as part of configuration management). * Defined vulnerability and patch processes to properly maintain new systems.   **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for restoring customer-deployed resources to a known operational state. The customer control implementation statement should address the customer-defined time period within which restoration must occur from configuration-controlled and integrity-protected information representing a known, operational state. Note: if the customer configures Microsoft Azure backup and/or alternate site processing services appropriately, Azure can support the continued operation of customer-deployed resources. |

## Identification and Authentication (IA)

### IA-1 Identification and Authentication Policy and Procedures (H)

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 annually]; and
   2. Identification and authentication procedures [FedRAMP Assignment: at least annually or whenever a significant change occurs].

| IA-1 | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter IA-1(a): *<Customer-defined personnel or roles>* | |
| Parameter IA-1(a): *<FedRAMP Assignment: at least annually>* | |
| Parameter IA-1(b)(1): *<FedRAMP Assignment: at least annually or whenever a significant change occurs>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| IA-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for developing, documenting, reviewing, updating, and disseminating identification and authentication policy and procedures for customer-deployed resources. The customer control implementation statement should address the content of the policy (which must include purpose, scope, roles, responsibilities, management commitment, coordination, and compliance), procedures (which must facilitate the implementation of the policies and associated controls), the frequency of review, and the role(s) responsible. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for developing, documenting, reviewing, updating, and disseminating identification and authentication policy and procedures for customer-deployed resources. The customer control implementation statement should address the content of the policy (which must include purpose, scope, roles, responsibilities, management commitment, coordination, and compliance), procedures (which must facilitate the implementation of the policies and associated controls), the frequency of review, and the role(s) responsible. |

### 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-2 | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-2 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for uniquely identifying and authenticating organizational users. The customer control implementation statement should address the mechanisms used to identify and authenticate users, both internal and external (if applicable), and any processes acting on behalf of the users. |

#### IA-2 (1) Control Enhancement (L) (M) (H)

The information system implements multifactor authentication for network access to privileged accounts.

| IA-2 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-2 (1) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for implementing multifactor authentication for network access to privileged accounts. The customer control implementation statement should address privileged account types and how multifactor authentication is enforced. |

#### IA-2 (2) Control Enhancement (M) (H)

The information system implements multifactor authentication for network access to non-privileged accounts.

| IA-2 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-2 (2) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for implementing multifactor authentication for network access to non-privileged accounts. The customer control implementation statement should address non-privileged account types and how multifactor authentication is enforced. |

#### IA-2 (3) Control Enhancement (M) (H)

The information system implements multifactor authentication for local access to privileged accounts.

| IA-2 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-2 (3) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure does not permit local access unless physical access is required. Local Administrator access must only be used to troubleshoot issues in instances where the member server is experiencing network issues and domain authentication is not working.  Azure implements multifactor authentication for local access via access control mechanisms required for physical access to the environment. Rooms within the Azure datacenters that contain all Azure Infrastructure systems within the system boundary are restricted through various physical security mechanisms, including the requirement for corporate smart card badging access and biometric devices. Both forms of authentication are required for physical access at the ingress point to Azure datacenter colocations.  **Customer Responsibility (IaaS/PaaS)**  Customers do not have local access to any system resources in Azure datacenters. All local access protection controls are implemented and managed by Microsoft Azure, and this control is inherited from Azure. |

#### IA-2 (4) Control Enhancement (H)

The information system implements multifactor authentication for local access to non-privileged accounts.

| IA-2 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-2 (4) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure considers all Microsoft Azure Government accounts used by Microsoft Azure Government personnel as privileged. Multifactor authentication is implemented for all Microsoft Azure Government personnel accounts using smartcards and pins, which includes local access.  **Customer Responsibility (IaaS/PaaS)**  Customers do not have local access to any system resources in Azure datacenters. All local access protection controls are implemented and managed by Microsoft Azure, and this control is inherited from Azure. |

#### 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-2 (5) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-2 (5) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for requiring individuals using group authenticators to first authenticate using individual authenticators. The customer control implementation statement should address the conditions under which group authenticators are used and the process through which individual authentication is associated with the use of the group authenticators. |

#### IA-2 (8) Control Enhancement (M) (H)

The information system implements replay-resistant authentication mechanisms for network access to privileged accounts.

| IA-2 (8) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-2 (8) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for implementing replay-resistant authentication mechanisms for network access to privileged accounts. The customer control implementation statement should address privileged account types and how replay-resistant authentication is implemented. |

#### IA-2 (9) Control Enhancement (H)

The information system implements replay-resistant authentication mechanisms for network access to non-privileged accounts.

| IA-2 (9) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-2 (9) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for implementing replay-resistant authentication mechanisms for network access to non-privileged accounts. The customer control implementation statement should address non-privileged account types and how replay-resistant authentication is implemented. |

#### 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-2 (11) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter IA-2(11): *<FedRAMP Assignment: FIPS 140-2, NIAP Certification, or NSA approval>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-2 (11) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for implementing multifactor authentication to access customer-deployed resources remotely. The customer control implementation statement should address how multifactor authentication is implemented for remote access, the requirement that one of the factors is provided by a device separate from the customer-deployed resources gaining access, and the customer-defined strength of mechanism requirements for the separate device. |

#### 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-2 (12) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-2 (12) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  Note: Personal Identity Verification (PIV) credentials are those credentials issued by federal agencies that conform to FIPS Publication 201 and supporting guidance documents. Customers will not be expected to perform this credential verification for government agencies. A mechanism for allowing government agencies to perform credential verification in a way that can be trusted by the customer system is through Active Directory Federation Services (ADFS). For more information about ADFS, see the following TechNet article: <https://technet.microsoft.com/en-us/magazine/dn250023.aspx>.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for accepting and verifying Personal Identity Verification (PIV) credentials. The customer control implementation statement should address the mechanisms for accepting and verifying PIV credentials. Note: if the customer does not deploy PIV credentials this control is not applicable. |

### 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-3 | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>*; Microsoft Azure | |
| Parameter IA-3-1: *<Customer-defined specific and/or types of devices>* | |
| Parameter IA-3-2: *<Selection (one or more): local, remote, 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-3 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure identifies and authenticates the following types of devices within the accreditation boundary: network devices, physical servers, virtual machines (including PaaS VMs).  As part of the network discovery and configuration steps in the bootstrap workflow, network devices are pre-configured to use DHCP/PXE boot for their configuration. Upon boot of the network device, the bootstrap agent provides the OS image for the device and the basic configuration, including the IP address and credentials, before establishing the connection to the environment.  All Microsoft Azure physical servers are joined to an Active Directory domain when deployed. Active Directory forest members are uniquely identified by Universally Unique Identifiers (UUIDs) and authenticated using NTLM v2 and Kerberos v5 as 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.  **Customer Responsibility (PaaS)**  PaaS resources do not permit device-level connections. Customers inherit this control for PaaS resources implemented on Microsoft Azure.  **Customer Responsibility (IaaS)**  The customer is responsible for implementing device identification and authentication. The customer control implementation statement should address customer-defined specific and/or types of devices and connections, as well as how devices are uniquely identified and authenticated prior to establishing a connection. |

### IA-4 Identifier Management (H)

The organization manages information system identifiers for users and devices by:

1. Receiving authorization from [FedRAMP Assignment at a minimum, the ISSO (or similar role within the organization)] to assign an individual, group, role, or device identifier;

Selecting an identifier that identifies an individual, group, role, or device;

Assigning the identifier to the intended individual, group, role, or device;

Preventing reuse of identifiers for [FedRAMP Assignment: at least two (2) years]; and

Disabling the identifier after [FedRAMP Assignment: thirty-five (35) days (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-defined>* | |
| Parameter IA-4(a): *<FedRAMP Assignment at a minimum, the ISSO (or similar role within the organization)>* | |
| Parameter IA-4(d): *<FedRAMP Assignment: at least two (2) years>* | |
| Parameter IA-4(e): *<FedRAMP Assignment: thirty-five (35) days (see additional requirements and guidance)>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for managing identifiers (i.e., individuals, groups, roles, and devices) for customer resources. The customer control implementation statement should address the requirement that authorization is provided by customer-defined personnel/roles prior to assigning identifiers. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for managing identifiers (i.e., individuals, groups, roles, and devices) for customer resources. The customer control implementation statement should address the selection of identifiers. |
| Part c | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for managing identifiers (i.e., individuals, groups, roles, and devices) for customer resources. The customer control implementation statement should address the assignment of identifiers. |
| Part d | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for managing identifiers (i.e., individuals, groups, roles, and devices) for customer resources. The customer control implementation statement should address the customer-defined time period during which identifier reuse is prevented. |
| Part e | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for managing identifiers (i.e., individuals, groups, roles, and devices) for customer resources. The customer control implementation statement should address the customer-defined time period of inactivity at which identifiers are disabled. |

#### IA-4 (4) Control Enhancement (M) (H)

The organization manages individual identifiers by uniquely identifying each individual as [FedRAMP Assignment: contractors; foreign nationals].

| IA-4 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter IA-4 (4): *<FedRAMP Assignment: contractors; foreign nationals>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-4 (4) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for identifying the status (e.g., contractor, foreign national) of individual users. The customer control implementation statement should address the management of identifiers by uniquely identifying each individual based upon customer-defined characteristics. |

### IA-5 Authenticator Management (H)

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;

Establishing initial authenticator content for authenticators defined by the organization;

Ensuring that authenticators have sufficient strength of mechanism for their intended use;

Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;

Changing default content of authenticators prior to information system installation;

Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;

Changing/refreshing authenticators [FedRAMP Assignment: to include sixty (60) days for passwords].

Protecting authenticator content from unauthorized disclosure and modification;

Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and

Changing authenticators for group/role accounts when membership to those accounts changes.

IA-5 Additional FedRAMP Requirements and Guidance:

Requirement: Authenticators must be compliant with NIST SP 800-63-2 Electronic Authentication Guideline assurance level 4. Link <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf>

| IA-5 | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter IA-5(g): *<FedRAMP Assignment: to include sixty (60) days for passwords>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for managing authenticators. The customer control implementation statement should address verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator (e.g., verifying an individual’s identity with a government-issued identification card). |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for managing authenticators. The customer control implementation statement should address establishing initial authenticator content for authenticators defined by the customer. |
| Part c | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for managing authenticators. The customer control implementation statement should address the requirement that authenticators have sufficient strength of mechanism for their intended use. |
| Part d | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for managing authenticators. The customer control implementation statement should address the requirement that the customer implements administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators. |
| Part e | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for managing authenticators. The customer control implementation statement should address changing default content of authenticators prior to deployment. |
| Part f | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for managing authenticators. The customer control implementation statement should address the establishment of minimum and maximum lifetime restrictions and reuse conditions for authenticators. |
| Part g | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for managing authenticators. The customer control implementation statement should address the requirement of changing/refreshing authenticators, and the corresponding time period for each authenticator type after which an update is required. |
| Part h | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for managing authenticators. The customer control implementation statement should address the requirement to protect authenticator content from unauthorized disclosure and modification. |
| Part i | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for managing authenticators. The customer control implementation statement should address the requirement for individuals to take, and devices to implement, specific security safeguards to protect authenticators. |
| Part j | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for managing authenticators. The customer control implementation statement should address the requirement of changing authenticators for group/role accounts when membership changes occur. |

#### IA-5 (1) Control Enhancement (H)

The information system, for password-based authentication:

1. Enforces minimum password complexity of [FedRAMP Assignment: case sensitive, minimum of fourteen (14) characters, and at least one (1) each of upper-case letters, lower-case letters, numbers, and special characters];

Enforces at least the following number of changed characters when new passwords are created: [FedRAMP Assignment: at least fifty percent (50%)];

Stores and transmits only cryptographically-protected passwords;

Enforces password minimum and maximum lifetime restrictions of [FedRAMP Assignment: one (1) day minimum, sixty (60) day maximum];

Prohibits password reuse for [FedRAMP Assignment: twenty-four (24)] generations; and

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-defined>* | |
| Parameter IA-5(1)(a): *<FedRAMP Assignment: case sensitive, minimum of fourteen (14) characters, and at least one (1) each of upper-case letters, lower-case letters, numbers, and special characters>* | |
| Parameter IA-5(1)(b): *<FedRAMP Assignment: at least fifty percent (50%)>* | |
| Parameter IA-5(1)(d): *<FedRAMP Assignment: one (1) day minimum, sixty (60) day maximum>* | |
| Parameter IA-5(1)(e): *<FedRAMP Assignment: twenty-four (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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-5 (1) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for employing password-based authentication within customer-deployed resources. The customer control implementation statement should address password complexity requirements (i.e., case sensitivity; number of characters; and the mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type), and the mechanism(s) used to enforce the requirements. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for employing password-based authentication within customer-deployed resources. The customer control implementation statement should address the customer-defined number of characters to be changed when new passwords are created. |
| Part c | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for employing password-based authentication within customer-deployed resources. The customer control implementation statement should address the requirement to only store and transmit cryptographically-protected passwords. |
| Part d | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for employing password-based authentication within customer-deployed resources. The customer control implementation statement should address the enforcement of customer-defined minimum and maximum password lifetime restrictions (e.g., new password must be used for a minimum of 10 days and must be changed within 60 days). |
| Part e | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for employing password-based authentication within customer-deployed resources. The customer control implementation statement should address the customer-defined number of password generations that are prohibited from reuse (e.g., 10 most recent passwords may not be reused when creating a new password). |
| Part f | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for employing password-based authentication within customer-deployed resources. The customer control implementation statement should address the customer's ability to issue users a temporary password with the requirement to immediately change to a permanent password 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-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-5 (2) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for employing PKI-based authentication within customer-deployed resources. The customer control implementation statement should address the requirement to validate certifications by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for employing PKI-based authentication within customer-deployed resources. The customer control implementation statement should address the enforcement of authorized access to private keys. |
| Part c | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for employing PKI-based authentication within customer-deployed resources. The customer control implementation statement should address the mapping of each authenticated identity to the account of the corresponding individual or group. |
| Part d | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for employing PKI-based authentication within customer-deployed resources. The customer control implementation statement should address the implementation of a local cache of private key data to support path discovery and validation when unable to access this information via the network. |

#### 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-5 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter IA-5(3)-1: *<FedRAMP Assignment: All hardware/biometric (multifactor authenticators)>* | |
| Parameter IA-5(3)-2: *<FedRAMP Selection: in person>* | |
| Parameter IA-5(3)-3: *<Customer-defined registration authority>* | |
| Parameter IA-5(3)-4: *<Customer-defined personnel or roles>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-5 (3) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for registering authenticators. The customer control implementation statement should address the types of and/or specific authenticators requiring in-person registration, customer-defined registration authority, and personnel/roles assigned to authorize registration. |

#### IA-5 (4) Control Enhancement (H)

The organization employs automated tools to determine if password authenticators are sufficiently strong to satisfy [FedRAMP Assignment: complexity as identified in IA-5 (1) Control Enhancement (H) Part A].

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-5 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter IA-5(4): *<FedRAMP Assignment: complexity as identified in IA-5 (1) Control Enhancement (H) Part A>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-5 (4) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for employing automated tools to validate password strength requirements. The customer control implementation statement should address the automated mechanisms used to determine if password authenticators are sufficiently strong to satisfy customer-defined password strength requirements. |

#### 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-5 (6) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-5 (6) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for protecting authenticators. The customer control implementation statement should address the mechanisms used to protect authenticators commensurate with the security category of the information to be accessed. |

#### 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-5 (7) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-5 (7) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for ensuring there are no unencrypted static authenticators within customer-deployed resources. The customer control implementation statement should address the mechanisms used to ensure unencrypted static authenticators are not embedded within customer applications/scripts or stored on function keys. |

#### IA-5 (8) Control Enhancement (H)

The organization implements [FedRAMP Assignment: different authenticators on different systems] to manage the risk of compromise due to individuals having accounts on multiple information systems.

| IA-5 (8) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter IA-5 (8): *<FedRAMP Assignment: different authenticators on different 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-5 (8) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for managing the risk imposed by users with multiple accounts on customer-deployed resources. The customer control implementation statement should address the security safeguards used to manage the risk of compromise due to individuals having accounts on multiple information systems (e.g., having different authenticators on all systems, employing some form of single sign-on mechanism, or including some form of one-time passwords on all systems). |

#### 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-5 (11) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter IA-5(11): *<Customer-defined token quality 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-5 (11) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for employing mechanisms to satisfy hardware token-based authentication quality requirements. The customer control implementation statement should address the customer-defined quality requirements in place. |

#### IA-5 (13) Control Enhancement (H)

The information system prohibits the use of cached authenticators after [Assignment: organization-defined time period].

| IA-5 (13) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter IA-5 (13): *<Customer-defined time period>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-5 (13) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for enforcing the expiration of cached authenticators. The customer control implementation statement should address the customer-defined time period after which the reuse of cached authenticators will be prohibited. |

### 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-6 | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-6 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for obscuring authentication feedback information during the authentication process for any customer-deployed resources. The customer control implementation statement should address the various authentication scenarios that might arise and the mechanism used to obscure feedback during each. |

### 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-7 | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-7 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for implementing mechanisms for authentication to a cryptographic module (e.g., configuring web applications). The customer control implementation statement should address how the selected encryption level satisfies the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. |

### 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-8 | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-8 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for identifying and authenticating non-organizational users accessing customer-deployed resources. The customer control implementation statement should address how non-organizational users (or processes acting on their behalf) are uniquely identified and authenticated (e.g., database for non-organizational users to log into a web application). |

#### 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-8 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-8 (1) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  Note: Personal Identity Verification (PIV) credentials are those credentials issued by federal agencies that conform to FIPS Publication 201 and supporting guidance documents. Customers will not be expected to perform this credential verification for government agencies. A mechanism for allowing government agencies to perform credential verification in a way that can be trusted by the customer system is through Active Directory Federation Services (ADFS). For more information about ADFS, see the following TechNet article: <https://technet.microsoft.com/en-us/magazine/dn250023.aspx>.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for accepting and verifying Personal Identity Verification (PIV) credentials issued by other federal agencies. The customer control implementation statement should address the mechanisms for accepting and verifying PIV credentials that have been issued by other government agencies. Note: if the customer does not deploy PIV credentials this control is not applicable. |

#### IA-8 (2) Control Enhancement (L) (M) (H)

The information system accepts only FICAM-approved third-party credentials.

| IA-8 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-8 (2) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  Note: FICAM approved credentials are those credentials issued by nonfederal government entities approved by the Federal Identity, Credential, and Access Management (FICAM) Trust Framework Solutions initiative. Customers will not be expected to perform this credential verification for government agencies. A mechanism for allowing government agencies to perform credential verification in a way that can be trusted by the customer system is through Active Directory Federation Services (ADFS).  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for only accepting third-party credentials that have been approved by the Federal Identity, Credential, and Access Management (FICAM) Trust Framework Solutions initiative. The customer control implementation statement should address the mechanisms for accepting FICAM-approved credentials. Note: if the customer’s deployed resources do not allow third-party credentials this control is not applicable. |

#### 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-8 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter IA-8(3): *<Customer-defined 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)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-8 (3) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  Note: FICAM approved credentials are those credentials issued by nonfederal government entities approved by the Federal Identity, Credential, and Access Management (FICAM) Trust Framework Solutions initiative. Customers will not be expected to perform this credential verification for government agencies. A mechanism for allowing government agencies to perform credential verification in a way that can be trusted by the customer system is through Active Directory Federation Services (ADFS).  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for employing only Federal Identity, Credential, and Access Management (FICAM) Trust Framework Solutions initiative approved resources for accepting third-party credentials. The customer control implementation statement should address the resources used in the customer-defined system for accepting FICAM-approved credentials. Note: if the customer’s deployed resources do not allow third-party credentials this control is not applicable. |

#### IA-8 (4) Control Enhancement (L) (M) (H)

The information system conforms to FICAM-issued profiles.

| IA-8 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-8 (4) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  Note: FICAM approved credentials are those credentials issued by nonfederal government entities approved by the Federal Identity, Credential, and Access Management (FICAM) Trust Framework Solutions initiative. Customers will not be expected to perform this credential verification for government agencies. A mechanism for allowing government agencies to perform credential verification in a way that can be trusted by the customer system is through Active Directory Federation Services (ADFS).  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for conforming to the profiles issued by the Federal Identity, Credential, and Access Management (FICAM) Trust Framework Solutions initiative. The customer control implementation statement should address how customer deployed resources conform to FICAM-issued profiles. Note: if the customer’s deployed resources do not allow third-party credentials this control is not applicable. |

## Incident Response (IR)

### IR-1 Incident Response Policy and Procedures (H)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and
2. Reviews and updates the current:
   1. Incident response policy [FedRAMP Assignment: at least annually]; and
   2. Incident response procedures [FedRAMP Assignment: at least annually or whenever a significant change occurs].

| IR-1 | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter IR-1(a): *<Customer-defined personnel or roles>* | |
| Parameter IR-1(b)(1): <FedRAMP Assignment: at least annually> | |
| Parameter IR-1(b)(2): <FedRAMP Assignment: at least annually or whenever a significant change occurs> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| IR-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for developing, documenting, reviewing, updating, and disseminating incident response policy and procedures for customer-deployed resources. The customer control implementation statement should address the content of the policy (which must include purpose, scope, roles, responsibilities, management commitment, coordination, and compliance), procedures (which must facilitate the implementation of the policies and associated controls), the frequency of review, and the role(s) responsible. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for developing, documenting, reviewing, updating, and disseminating incident response policy and procedures for customer-deployed resources. The customer control implementation statement should address the content of the policy (which must include purpose, scope, roles, responsibilities, management commitment, coordination, and compliance), procedures (which must facilitate the implementation of the policies and associated controls), the frequency of review, and the role(s) responsible. |

### IR-2 Incident Response Training (H)

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 [FedRAMP Assignment: ten (10) days] of assuming an incident response role or responsibility;
2. When required by information system changes; and
3. [FedRAMP Assignment: at least annually] thereafter.

| IR-2 | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter IR-2(a): <FedRAMP Assignment: ten (10) days> | |
| Parameter IR-2(c): <FedRAMP Assignment: 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IR-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for providing incident response training to users of customer-deployed resources in accordance with assigned roles and responsibilities. The customer control implementation statement should address the time period within which personnel assuming an incident response role/responsibility must be trained. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for providing incident response retraining to users of customer-deployed resources, when changes occur, in accordance with assigned roles and responsibilities. The customer control implementation statement should address the types of changes to customer-deployed resources that necessitate retraining. |
| Part c | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for providing incident response retraining to users of customer-deployed resources, as required, in accordance with assigned roles and responsibilities. The customer control implementation statement should address the customer-defined frequency with which retraining is required. |

#### IR-2 (1) Control Enhancement (H)

The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.

| IR-2 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IR-2 (1) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for providing incident response training, which incorporates simulated events, to users of customer-deployed resources in accordance with assigned roles and responsibilities. The customer control implementation statement should address the simulated events included in incident response training. |

#### IR-2 (2) Control Enhancement (H)

The organization employs automated mechanisms to provide a more thorough and realistic incident response training environment.

| IR-2 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IR-2 (2) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for providing incident response training, which employs automated mechanisms, to users of customer-deployed resources in accordance with assigned roles and responsibilities. The customer control implementation statement should address the automated mechanisms that provide a more through and realistic training environment. |

### IR-3 Incident Response Testing (H)

The organization tests the incident response capability for the information system [FedRAMP Assignment: at least every six (6) months] 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-3 | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter IR-3-1: <FedRAMP Assignment: at least every six (6) months> | |
| Parameter IR-3-2: <FedRAMP Assignment: *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.*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IR-3 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for testing the incident response capability of customer-deployed resources. The customer control implementation statement should address the frequency within which testing occurs, the customer-defined tests used to determine incident response effectiveness, and the documentation of testing results. |

#### IR-3 (2) Control Enhancement (M) (H)

The organization coordinates incident response testing with organizational elements responsible for related plans.

| IR-3 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IR-3 (2) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for coordinating incident response testing with related plans. The customer control implementation statement should address the coordination of incident response testing with organizational elements responsible for related plans (e.g., business continuity, contingency, disaster recovery). |

### 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: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IR-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for implementing an incident handling capability. The customer control implementation statement should address key incident handling capabilities including preparation, detection and analysis, containment, eradication, and recovery. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for implementing an incident handling capability. The customer control implementation statement should address coordination of incident handling activities with contingency planning activities. |
| Part c | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for implementing an incident handling capability. The customer control implementation statement should address lessons learned from ongoing incident handling activities; their incorporation into incident response procedures, training, and testing going forward; and the implementation of the resulting changes. |

#### IR-4 (1) Control Enhancement (M) (H)

The organization employs automated mechanisms to support the incident handling process.

| IR-4 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IR-4 (1) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for employing automated incident handling mechanisms. The customer control implementation statement should address the mechanisms in place to support the incident handling process (e.g., ticketing systems and incident tracking/reporting systems). |

#### IR-4 (2) Control Enhancement (H)

The organization includes dynamic reconfiguration of [FedRAMP Assignment: all network, data storage, and computing devices] as part of the incident response capability.

| IR-4 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter IR-4 (2): <FedRAMP Assignment: all network, data storage, and computing devices> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IR-4 (2) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for including dynamic reconfiguration of all customer-deployed resources as part of the incident response capability (e.g., filter rules to firewalls and gateways, access control lists). The customer control implementation statement should address the customer-defined resources capable of dynamic reconfiguration. |

#### IR-4 (3) Control Enhancement (H)

The organization identifies [Assignment: organization-defined classes of incidents] and [Assignment: organization-defined actions to take in response to classes of incident] to ensure continuation of organizational missions and business functions.

| IR-4 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter IR-4 (3)-1: *<Customer-defined classes of incidents>* | |
| Parameter IR-4 (3)-2: *<Customer-defined actions to take in response to classes of 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IR-4 (3) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for identifying classes of incidents and the actions taken in response to those incidents. The customer control implementation statement should address the customer-defined classes of incidents, and the actions taken in response to each class to ensure continuation of organizational missions and business functions. |

#### IR-4 (4) Control Enhancement (H)

The organization correlates incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.

| IR-4 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IR-4 (4) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for correlating incident information and individual incident responses across the customer organization in order to achieve perspective on incident awareness and response. The customer control implementation statement should address the correlation of incident information and individual responses which provide an organization-wide perspective on incident awareness. |

#### IR-4 (6) Control Enhancement (H)

The organization implements incident handling capability for insider threats.

| IR-4 (6) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IR-4 (6) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for implementing an incident handling capability for insider threats. The customer control implementation statement should address the customer's capability to handle insider threats. |

#### IR-4 (8) Control Enhancement (H)

The organization implements incident handling capability for insider threats.

The organization coordinates with [FedRAMP Assignment: external organizations including consumer incident responders and network defenders and the appropriate consumer incident response team (CIRT)/ Computer Emergency Response Team (CERT) (such as US-CERT, DoD CERT, IC CERT)] to correlate and share [Assignment: organization-defined incident information] to achieve a cross- organization perspective on incident awareness and more effective incident responses.

| IR-4 (8) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter IR-4 (8)-1: <FedRAMP Assignment: external organizations including consumer incident responders and network defenders and the appropriate consumer incident response team (CIRT)/ Computer Emergency Response Team (CERT) (such as US-CERT, DoD CERT, IC CERT)> | |
| Parameter IR-4 (8)-2: *<Customer-defined incident 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IR-4 (8) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for coordinating with external organizations to achieve a cross-organizational perspective on incident awareness and more effective incident responses. The customer control implementation statement should address the customer-defined external organizations and incident information to be shared. |

### IR-5 Incident Monitoring (L) (M) (H)

The organization tracks and documents information system security incidents.

| IR-5 | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IR-5 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for incident monitoring. The customer control implementation statement should address the mechanisms used for tracking and documenting security incidents for customer-deployed resources. |

#### IR-5 (1) Control Enhancement (H)

The organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.

| IR-5 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text., Date of Authorization | |

| IR-5 (1) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for employing automated mechanisms to assist in incident monitoring. The customer control implementation statement should address the mechanisms employed for tracking security incidents and collecting/analyzing incident information. |

### 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: *<Customer-defined>* | |
| Parameter IR-6(a): *<*FedRAMP Assignment: US-CERT incident reporting timelines as specified in NIST SP800-61 (as amended)> | |
| Parameter IR-6(b): *<Customer-defined authorities>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IR-6 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for requiring personnel to report suspected security incidents to the organizational incident response capability. The customer control implementation statement should address the timeframe within which incidents must be reported. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for reporting security incident information. The customer control implementation statement should address the customer-defined authorities to be notified. Note: in cases where customer security incidents may affect the security status of Microsoft Azure, the customer is responsible for notifying Microsoft Azure. Additionally, customers who are classified as a government agency is responsible to designate US-CERT as a notification contact. |

#### IR-6 (1) Control Enhancement (M) (H)

The organization employs automated mechanisms to assist in the reporting of security incidents.

| IR-6 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IR-6 (1) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for employing automated mechanisms to support incident reporting. The customer control implementation statement should address the mechanisms used (e.g., ticketing and incident tracking/reporting systems) to assist in the reporting of security incidents. |

### 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-7 | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IR-7 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for providing incident response support resources that are integral to the organizational incident response capability. The customer control implementation statement should address the customer's capability to offer advice and assistance to users for the handling and reporting of security incidents. |

#### IR-7 (1) Control Enhancement (M) (H)

The organization employs automated mechanisms to increase the availability of incident response related information and support.

| IR-7 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IR-7 (1) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for using automated mechanisms to increase the availability of incident response support resources. The customer control implementation statement should address the support mechanisms used. |

#### 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: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IR-7 (2) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for establishing relationships between its incident response capability and external providers. The customer control implementation statement should address the external relationships which provide resource protection. Note: it is the customer’s responsibility to provide accurate and current contact information to Microsoft Azure in order to receive notifications of security incidents involving the potential breach of customer data. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for identifying incident response team members to Microsoft Azure and any other external providers. The customer control implementation statement should address the team members. |

### 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: *<Customer-defined>* | |
| Parameter IR-8(a)(8): *<Customer-defined personnel or roles>* | |
| Parameter IR-8(b): *<*FedRAMP Assignment: *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.*> | |
| Parameter IR-8(c): *<*FedRAMP Assignment: at least annually> | |
| Parameter IR-8(e): *<FedRAMP Assignment: 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.>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IR-8 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for developing an incident response plan for customer-deployed resources. The customer control implementation statement should address the inclusion of following in the incident response plan: a roadmap for implementing its incident response capability; the structure and organization of the incident response capability; a high-level approach for how incident response fits into the customer's organization; how the plan meets unique customer requirements which relate to mission, size, structure and functions; a definition of reportable incidents; metrics for measuring incident response capability; resources and management support needed to effectively maintain and mature the incident response capability; and the personnel/roles responsible for reviewing and approving the plan. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for distributing the incident response plan. The customer control implementation statement should address the key personnel (identified by name and/or role) and customer elements who should receive a copy of the incident response plan defined in IR-08.a. |
| Part c | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for reviewing the incident response plan. The customer control implementation statement should address the frequency with which the incident response plan is reviewed. |
| Part d | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for updating the incident response plan. The customer control implementation statement should address how updates reflect changes to the organization, resources, or environment of operation; and the problems encountered during implementation, execution, or testing of incident response activities. |
| Part e | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for communicating changes made to the incident response plan. The customer control implementation statement should address the means by which the customer communicates changes to the key personnel defined in IR-08.b. |
| Part f | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for protecting the incident response plan. The customer control implementation statement should address the process for preventing unauthorized disclosure or modification of the plan. |

### 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: *<Customer-defined>* | |
| Parameter IR-9(b): *<Customer-defined personnel or roles>* | |
| Parameter IR-9(f): *<Customer-defined 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IR-9 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for responding to information spills. The customer control implementation statement should address the specific information involved in the information contamination. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for responding to information spills. The customer control implementation statement should address the personnel/roles to be alerted of the information spill and the usage of a communication method that is not associated with the spill. |
| Part c | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for responding to information spills. The customer control implementation statement should address how the contaminated customer-deployed resources are isolated. |
| Part d | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for responding to information spills. The customer control implementation statement should address the eradication of information from the contaminated resources. |
| Part e | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for responding to information spills. The customer control implementation statement should address the identification of other resources which may have been subsequently contaminated. |
| Part f | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for responding to information spills. The customer control implementation statement should address any other customer-defined actions to be performed. |

#### IR-9 (1) Control Enhancement (M) (H)

The organization assigns [Assignment: organization-defined personnel or roles] with responsibility for responding to information spills.

| IR-9 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter IR-9(1): *<Customer-defined personnel or roles>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IR-9 (1) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for assigning individuals for responding to information spills. The customer control implementation statement should address the personnel/roles tasked with responding to information spills. |

#### IR-9 (2) Control Enhancement (H)

The organization provides information spillage response training [FedRAMP Assignment: at least annually].

| IR-9 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter IR-9(2): *<FedRAMP Assignment: 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IR-9 (2) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for providing information spillage response training. The customer control implementation statement should address the frequency with which information spillage training is provided. |

#### 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-9 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter IR-9(3): *<Customer-defined procedures>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IR-9 (3) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for ensuring customer personnel impacted by information spills can continue carrying out assigned tasks. The customer control implementation statement should address the customer-defined procedures to be implemented while contaminated resources are undergoing corrective actions. |

#### 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-9 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter IR-9(4): *<Customer-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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IR-9 (4) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for managing exposure of spilled information to unauthorized personnel. The customer control implementation statement should address the customer-defined security safeguards employed for personnel exposed to information not within assigned access authorizations. |

## Maintenance (MA)

### MA-1 System Maintenance Policy and Procedures (H)

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 annually]; and
   2. System maintenance procedures [FedRAMP Assignment: at least annually or whenever a significant change occurs].

| MA-1 | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter MA-1(a): *<Customer-defined personnel or roles>* | |
| Parameter MA-1(b)(1): *<FedRAMP Assignment: at least annually>* | |
| Parameter MA-1(b)(2): < FedRAMP Assignment: at least annually or whenever a significant change occurs> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| MA-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for developing, documenting, reviewing, updating, and disseminating system maintenance policy and procedures for the customer-deployed resources. The customer control implementation statement should address the content of the policy (which must include purpose, scope, roles, responsibilities, management commitment, coordination, and compliance), procedures (which must facilitate the implementation of the policies and associated controls), the frequency of review, and the role(s) responsible. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for developing, documenting, reviewing, updating, and disseminating system maintenance policy and procedures for the customer-deployed resources. The customer control implementation statement should address the content of the policy (which must include purpose, scope, roles, responsibilities, management commitment, coordination, and compliance), procedures (which must facilitate the implementation of the policies and associated controls), the frequency of review, and the role(s) responsible. |

### 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: *<Customer-defined>;* Microsoft Azure | |
| Parameter MA-2(c): *<Customer-defined personnel or roles>;* Datacenter Management, Property asset owners | |
| Parameter MA-2(f): *<Customer-defined maintenance-related information>;* (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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| MA-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure schedules, performs, documents and reviews records of maintenance on all Azure components. Teams use computerized maintenance management systems to manage maintenance schedules and work order management. Each team schedules, performs, documents, and reviews maintenance activities using the appropriate maintenance management system.  **Customer Responsibility (PaaS)**  Customers do not have access to perform system maintenance for resources deployed to PaaS virtual machines; all physical maintenance and repair controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure.  **Customer Responsibility (IaaS)**  The customer is responsible for controlled maintenance. The customer control implementation statement should address the scheduling, performing, documenting and reviewing of remote maintenance and repair records for all customer-deployed operating systems in accordance with organizational requirements. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure performs maintenance in areas of the datacenter that are controlled and protected by physical security mechanisms (e.g., approved access, cameras, 2FA: access badges, biometrics, security patrols). Maintenance activities are managed using computerized maintenance management systems.  **Customer Responsibility (PaaS)**  Customers do not have access to perform system maintenance for resources deployed to PaaS virtual machines; all physical maintenance and repair controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure.  **Customer Responsibility (IaaS)**  The customer is responsible for controlled maintenance. The customer control implementation statement should address the approval and monitoring of all remote maintenance activities performed on customer-deployed operating systems. |
| Part c | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure requires that property assets (e.g., network device or server) requiring transfer offsite have explicit asset owner approval.  **Customer Responsibility (IaaS/PaaS)**  Customers do not have physical access to remove system resources from Azure datacenters to off-site maintenance or repair facilities; all physical maintenance and repair controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure. |
| Part d | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure's Asset Protection Standard defines the asset handling precautions required for offsite transfer of assets. The Asset Protection Standard requires that data storage assets be cleared/purged in a manner consistent with NIST SP 800-88, Guidelines for Media Sanitization, prior to leaving the datacenter.  **Customer Responsibility (IaaS/PaaS)**  Customers do not have physical access to remove system resources from Azure datacenters to off-site maintenance or repair facilities. All physical maintenance and repair controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure. |
| Part e | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure requires that maintenance activities to undergo peer review as a verification of completeness and quality assurance. The peer reviews verify that any required configurations or security settings are correctly in place before completion of the maintenance.  **Customer Responsibility (PaaS)**  Customers do not have access to perform system maintenance for resources deployed to PaaS virtual machines; all physical maintenance and repair controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure.  **Customer Responsibility (IaaS)**  The customer is responsible for controlled maintenance. The customer control implementation statement should address the process for identifying potentially impacted security controls and the process used for verifying those controls are still functioning properly following maintenance/repair activities. |
| Part f | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure Datacenter Management retains the following information in the organizational maintenance records: the date and time of maintenance; name of the individual performing the maintenance; name of escort, if necessary; a description of the maintenance performed; and a list of equipment removed or replaced (including identification numbers, if applicable).  **Customer Responsibility (PaaS)**  Customers do not have access to perform system maintenance for resources deployed to PaaS virtual machines; all physical maintenance and repair controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure.  **Customer Responsibility (IaaS)**  The customer is responsible for controlled maintenance. The customer control implementation statement should address the inclusion of customer-defined maintenance-related information in organizational maintenance records. |

#### MA-2 (2) Control Enhancement (H)

The organization:

1. Employs automated mechanisms to schedule, conduct, and document maintenance and repairs; and
2. Produces up-to date, accurate, and complete records of all maintenance and repair actions requested, scheduled, in process, and completed.

| MA-2 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>;* Microsoft 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 FedRAMP Authorization for Click here to enter text. Date of Authorization | |

| MA-2 (2) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  Azure datacenters rely on a computerized maintenance management system to manage maintenance schedules and work order management.  All Site Services work on Azure assets are scheduled, performed, documented, and reviewed in work tickets within the workflow ticketing tool. No work can occur without an approved work ticket.  **Customer Responsibility (PaaS)**  Customers do not have access to perform system maintenance for resources deployed to PaaS virtual machines; all physical maintenance and repair controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure.  **Customer Responsibility (IaaS)**  The customer is responsible for automating maintenance activities. The customer control implementation statement should address how automated mechanisms are used to schedule, conduct, and document maintenance and repairs of customer-deployed operating systems. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure utilizes a maintenance ticketing tracking tool to document and track all maintenance on CE equipment.  All Site Services work on Azure assets are scheduled, performed, documented, and reviewed in work tickets within the workflow ticketing tool.  **Customer Responsibility (PaaS)**  Customers do not have access to perform system maintenance for resources deployed to PaaS virtual machines; all physical maintenance and repair controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure.  **Customer Responsibility (IaaS)**  The customer is responsible for automating maintenance activities. The customer control implementation statement should address the production of up-to date, accurate, and complete records of all maintenance and repair actions requested, scheduled, in process, and completed for customer-deployed operating systems. |

### MA-3 Maintenance Tools (M) (H)

The organization approves, controls, and monitors information system maintenance tools.

| MA-3 | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>;* Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| MA-3 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure utilizes several tools to complete maintenance. Software maintenance tools are approved, controlled and maintained through the Microsoft Azure change and release process.  The Site Services team maintains an inventory of approved maintenance tools for use within the datacenter (see MA-3). Maintenance personnel are directed to use the provided maintenance tools. Datacenter management approval is required in order to use tools not provided by the datacenter. Physical hand tools (screwdrivers, wrenches, etc.) are exempt from this control.  Each facility contains a restricted physical lock box or access-controlled room for the storage of specialized maintenance tools, such as fluke ether scopes, fluke fiber channel testers, Ethernet toners, etc. The Site Services team performs routine inventory checks to verify the status of all tools. Access to lock box or maintenance storage room is tracked in the access badge reader logs, which are available in the event of an investigation.  **Customer Responsibility (PaaS)**  Customers do not have access to perform system maintenance for resources deployed to PaaS virtual machines; all physical maintenance and repair controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure.  **Customer Responsibility (IaaS)**  The customer is responsible for system maintenance tools used on customer-deployed operating systems. The customer control implementation statement should address how maintenance tools are approved, controlled, and monitored. |

#### 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-3 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| MA-3 (1) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure's Site Services team maintains an inventory of approved maintenance tools for use within the datacenter (see MA-3 for further details). Maintenance personnel are directed to use the provided maintenance tools. DCM approval is required in order to use tools not provided by the datacenter.  **Customer Responsibility (IaaS/PaaS)**  Customers do not have physical access to Azure datacenters, therefore they do not have the ability to manage maintenance tools as they enter the datacenter. All physical maintenance and repair controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure. |

#### 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-3 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>;* Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| MA-3 (2) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure prohibits the use of mobile computing or storage media in the production environment of Microsoft Azure datacenters without datacenter management approval. Use of personally owned media is prohibited from being used in the production environment of Microsoft Azure datacenters.  Microsoft Azure has implemented a process to inspect laptops prior to being used in the production environment of Microsoft Azure datacenters. Security officers are trained to challenge personnel using laptops in the production environment to verify that the laptops have undergone and passed inspection.  **Customer Responsibility (PaaS)**  Customers do not have access to perform system maintenance for resources deployed to PaaS virtual machines; all physical maintenance and repair controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure.  **Customer Responsibility (IaaS)**  The customer is responsible for checking media containing maintenance diagnostic and test programs prior to deployment on customer-deployed operating systems. The customer control implementation statement should address the process for checking media for malicious code. |

#### 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: Microsoft Azure | |
| Parameter MA-3(3)(d): Datacenter Management, Property asset owners | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| MA-3 (3) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure employs datacenter specific maintenance tools that are retained within the facility and are not removed. Each facility contains a restricted physical lock box or storage room that stores maintenance tools, such as fluke ether scopes, fluke fiber channel testers, Ethernet toners, etc. Access is controlled to the lock box or storage room in DCAT to prohibit unauthorized access to the maintenance tools.  Organizational information is protected during maintenance by the controls in MA-4. To access organizational information, the user must have privileged accounts and authenticators.  **Customer Responsibility (IaaS/PaaS)**  Customers do not have physical access to Azure datacenters, therefore they do not have the ability to manage physical maintenance tools and equipment. All physical maintenance and repair controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure employs datacenter specific maintenance tools that are retained within the facility and are not removed. Each facility contains a restricted physical lock box or storage room that stores maintenance tools, such as fluke ether scopes, fluke fiber channel testers, Ethernet toners, etc. Access is controlled to the lock box or storage room in DCAT to prohibit unauthorized access to the maintenance tools.  Organizational information is protected during maintenance by the controls in MA-4. To access organizational information, the user must have privileged accounts and authenticators.  **Customer Responsibility (IaaS/PaaS)**  Customers do not have physical access to Azure datacenters, therefore they do not have the ability to manage physical maintenance tools and equipment. All physical maintenance and repair controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure. |
| Part c | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure employs datacenter specific maintenance tools that are retained within the facility and are not removed. Each facility contains a restricted physical lock box or storage room that stores maintenance tools, such as fluke ether scopes, fluke fiber channel testers, Ethernet toners, etc. Access is controlled to the lock box or storage room in DCAT to prohibit unauthorized access to the maintenance tools.  Organizational information is protected during maintenance by the controls in MA-4. To access organizational information, the user must have privileged accounts and authenticators.  **Customer Responsibility (IaaS/PaaS)**  Customers do not have physical access to Azure datacenters, therefore they do not have the ability to manage physical maintenance tools and equipment. All physical maintenance and repair controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure. |
| Part d | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure employs datacenter specific maintenance tools that are retained within the facility and are not removed. Each facility contains a restricted physical lock box or storage room that stores maintenance tools, such as fluke ether scopes, fluke fiber channel testers, Ethernet toners, etc. Access is controlled to the lock box or storage room in DCAT to prohibit unauthorized access to the maintenance tools.  Organizational information is protected during maintenance by the controls in MA-4. To access organizational information, the user must have privileged accounts and authenticators.  **Customer Responsibility (IaaS/PaaS)**  Customers do not have physical access to Azure datacenters, therefore they do not have the ability to manage physical maintenance tools and equipment. All physical maintenance and repair controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure. |

### 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: *<Customer-defined>;* Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | | |
| MA-4 What is the solution and how is it implemented? | | |
| Part a | **Microsoft Azure (PaaS)**  Microsoft Azure adheres to Microsoft’s corporate SDL process, which requires all development teams to define and publish a list of approved tools and their associated security checks. This list is approved by the security advisor for the project team.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (PaaS)**  Customers do not have access to perform system maintenance for resources deployed to PaaS virtual machines; all physical maintenance and repair controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure.  **Customer Responsibility (IaaS)**  The customer is responsible for performing non-local maintenance on customer-deployed operating systems. The customer control implementation statement should address the approval and monitoring of non-local maintenance and diagnostic activities. | |
| Part b | **Microsoft Azure (PaaS)**  Microsoft Azure allows remote maintenance to be performed by only authorized Microsoft Azure employees.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (PaaS)**  Customers do not have access to perform system maintenance for resources deployed to PaaS virtual machines; all physical maintenance and repair controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure.  **Customer Responsibility (IaaS)**  The customer is responsible for performing non-local maintenance on customer-deployed operating systems. The customer control implementation statement should address the requirement that non-local maintenance and diagnostic tools are consistent with organizational policy and documented in the security plan. | |
| Part c | **Microsoft Azure (PaaS)**  Microsoft Azure enforces strong identification and authentication controls in conducting remote maintenance and diagnostic activities. Authentication is handled by AD using Gemalto smartcards.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (PaaS)**  Customers do not have access to perform system maintenance for resources deployed to PaaS virtual machines; all physical maintenance and repair controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure.  **Customer Responsibility (IaaS)**  The customer is responsible for performing non-local maintenance on customer-deployed operating systems. The customer control implementation statement should address the use of strong authenticators when establishing non-local maintenance and diagnostic sessions. | |
| Part d | **Microsoft Azure (PaaS)**  Microsoft Azure uses the RMA tool to audit the maintenance and changes performed on Microsoft Azure hardware. The RMA tool also monitors and tracks user activity.  Auditing of maintenance and diagnostics within the Microsoft Azure environment is performed via the TFS system as part of the JIT elevation process.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (PaaS)**  Customers do not have access to perform system maintenance for resources deployed to PaaS virtual machines; all physical maintenance and repair controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure.  **Customer Responsibility (IaaS)**  The customer is responsible for performing non-local maintenance on customer-deployed operating systems. The customer control implementation statement should address the requirement to maintain records for non-local maintenance and diagnostic activities. | |
| Part e | **Microsoft Azure (PaaS)**  Microsoft Azure terminates remote sessions after the just-in-time (JIT) elevation period expires.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (PaaS)**  Customers do not have access to perform system maintenance for resources deployed to PaaS virtual machines; all physical maintenance and repair controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure.  **Customer Responsibility (IaaS)**  The customer is responsible for performing non-local maintenance on customer-deployed operating systems. The customer control implementation statement should address the termination of session and network connections when non-local maintenance is completed. | |

#### 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-4 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>;* Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| MA-4 (2) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (PaaS)**  Microsoft Azure documents the installation and use of remote maintenance and diagnostic connections in the Microsoft Azure SSP for all asset types.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (PaaS)**  Customers do not have access to perform system maintenance for resources deployed to PaaS virtual machines; all physical maintenance and repair controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure.  **Customer Responsibility (IaaS)**  The customer is responsible for documenting non-local maintenance in the security plan for customer-deployed operating systems. The customer control implementation statement should address the documentation of policies and procedures for the establishment and use of non-local maintenance and diagnostic connections. |

#### MA-4 (3) Control Enhancement (H)

The organization:

1. Requires that nonlocal maintenance and diagnostic services be performed from an information system that implements a security capability comparable to the capability implemented on the system being serviced; or
2. Removes the component to be serviced from the information system prior to nonlocal maintenance or diagnostic services, sanitizes the component (with regard to organizational information) before removal from organizational facilities, and after the service is performed, inspects and sanitizes the component (with regard to potentially malicious software) before reconnecting the component to the information system.

| MA-4 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>;* Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| MA-4 (3) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure performs remote maintenance and diagnostic services by first logging in via RDP to a Jumpbox from a computer on Microsoft CorpNet, and then initiating a second RDP session from the Jumpbox to the destination server. No direct connection is possible from an employee’s computer to the destination server. Jumpboxes are within the Microsoft Azure boundary and are protected using the same safeguards as the rest of the system. TLS 1.2 is used to protect RDP connections.  **Customer Responsibility (PaaS)**  Customers do not have access to perform system maintenance for resources deployed to PaaS virtual machines; all physical maintenance and repair controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure.  **Customer Responsibility (IaaS)**  The customer is responsible for performing all non-local maintenance of customer-deployed operating systems from an information system that has comparable security. The customer control implementation statement should address the security capabilities of information systems used to perform non-local maintenance and diagnostic services. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure performs remote maintenance and diagnostic services by first logging in via RDP to a Jumpbox from a computer on Microsoft CorpNet, and then initiating a second RDP session from the Jumpbox to the destination server. No direct connection is possible from an employee’s computer to the destination server. Jumpboxes are within the Microsoft Azure boundary and are protected using the same safeguards as the rest of the system. TLS 1.2 is used to protect RDP connections.  **Customer Responsibility (PaaS)**  Customers do not have access to perform system maintenance for resources deployed to PaaS virtual machines; all physical maintenance and repair controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure.  **Customer Responsibility (IaaS)**  The customer is responsible for performing all non-local maintenance of customer-deployed operating systems from an information system that has comparable security. The customer control implementation statement should address the security capabilities of information systems used to perform non-local maintenance and diagnostic services. |

#### MA-4 (6) Enhancement (H)

The information system implements cryptographic mechanisms to protect the integrity and confidentiality of nonlocal maintenance and diagnostic communications.

| MA-4 (6) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>;* Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| MA-4 (6) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure ensures that all non-local maintenance and diagnostic connections to the Microsoft Azure Government environment follow the remote access requirements as outlined in Microsoft Azure’s Access Control SOP. Two-factor authentication is enforced using GSGO issued USME smart cards and PINS for remote access connections via the USME Remote Desktop Gateways. This is enforced through the configuration of the Remote Desktop servers and is audited through security monitoring tools. FIPS 140-2 SSLv3/TLSv1/v1.2 encryption is the required configuration for establishing remote connection to the USME Remote Desktop Gateway service.  **Customer Responsibility (PaaS)**  Customers do not have access to perform system maintenance for resources deployed to PaaS virtual machines; all physical maintenance and repair controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure.  **Customer Responsibility (IaaS)**  The customer is responsible for implementing cryptographic mechanisms when performing non-local maintenance and diagnostics of customer-deployed operating systems. The customer control implementation statement should address the cryptographic mechanisms used to protect the integrity and confidentiality of non-local maintenance and diagnostic communications. |

### 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: *<Customer-defined>;* Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| MA-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure manages maintenance personnel authorization for physical access to Microsoft Azure datacenters through a computerized system. Logical access (any non-local maintenance) is managed through the CM process and access is documented, provisioned, and approved as documented in AC-2.  **Customer Responsibility (PaaS)**  Customers do not have access to perform system maintenance for resources deployed to PaaS virtual machines; all physical maintenance and repair controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure.  **Customer Responsibility (IaaS)**  The customer is responsible for managing maintenance personnel. The customer control implementation statement should address the process for authorizing maintenance personnel and maintaining a list of authorized maintenance organizations/personnel. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure manages physical access authorizations for maintenance personnel in a computerized system. Teams have certification requirements that ensure their team members are knowledgeable in supporting their respective datacenter environments.  **Customer Responsibility (PaaS)**  Customers do not have access to perform system maintenance for resources deployed to PaaS virtual machines; all physical maintenance and repair controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure.  **Customer Responsibility (IaaS)**  The customer is responsible for managing maintenance personnel. The customer control implementation statement should address the requirement that non-escorted personnel performing maintenance on customer-deployed operating systems have the required access authorizations. |
| Part c | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure enforces that in the event that a vendor is required to perform maintenance, the vendor is escorted by someone who possesses the technical competence to supervise the work.  **Customer Responsibility (PaaS)**  Customers do not have access to perform system maintenance for resources deployed to PaaS virtual machines; all physical maintenance and repair controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure.  **Customer Responsibility (IaaS)**  The customer is responsible for managing maintenance personnel. The customer control implementation statement should address the designation of 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 (1) Control Enhancement (H)

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) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>;* Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| MA-5 (1) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure enforces that in the event that non-cleared personnel are required to perform maintenance, non-cleared personnel are escorted by cleared personnel who possess the technical competence to supervise the work. 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.  **Customer Responsibility (PaaS)**  Customers do not have access to perform system maintenance for resources deployed to PaaS virtual machines; all physical maintenance and repair controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure.  **Customer Responsibility (IaaS)**  The customer is responsible for managing the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens. The customer control implementation statement should address the following requirements regarding maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals: such personnel are escorted and supervised during maintenance and diagnostic activities on customer-deployed operating systems by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified; and all volatile information storage media within customer-deployed operating systems are sanitized and all non-volatile storage media are removed or disconnected from customer-deployed resources and secured prior to such personnel performing maintenance and diagnostic activities. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure enforces that in the event that non-cleared personnel are required to perform maintenance, non-cleared personnel are escorted by cleared personnel who possess the technical competence to supervise the work. 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.  **Customer Responsibility (PaaS)**  Customers do not have access to perform system maintenance for resources deployed to PaaS virtual machines; all physical maintenance and repair controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure.  **Customer Responsibility (IaaS)**  The customer is responsible for implementing alternate security safeguards for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens. The customer control implementation statement should address the safeguards implemented in the event that resources identified MA-05(01).a cannot be sanitized, removed, or disconnected from customer-deployed operating systems. |

### 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-6 | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>;* Microsoft Azure | |
| Parameter MA-6(1): *<Customer-defined information system components>;* Critical components list | |
| Parameter MA-6(2): *<Customer-defined time period>;* 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| MA-6 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft datacenters maintain resident maintenance personnel to support critical datacenter infrastructure systems as well as datacenter operations. The teams have identified critical security and technology system components which they maintain spares for onsite. Critical systems are designed in N+1 configurations and services are designed to be resilient. This allows the datacenter management team to meet recovery goals in the event of a service interruption or contingency plan situation. Critical information system services are provisioned from more than one datacenter to prevent an interruption in service due to an incident at one of the datacenters. Customer applications are responsible for deploying to multiple datacenters to provide for redundancy and resiliency.  **Customer Responsibility (PaaS)**  Customers do not have access to perform system maintenance for resources deployed to PaaS virtual machines; all physical maintenance and repair controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure.  **Customer Responsibility (IaaS)**  The customer is responsible for timely maintenance support. The customer control implementation statement should address time period after resource failure within which the customer should obtain maintenance support for customer-deployed operating systems. |

## Media Protection (MP)

### MP-1 Media Protection Policy and Procedures (H)

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 annually]; and
   2. Media protection procedures [FedRAMP Assignment: at least annually or whenever a significant change occurs].

| MP-1 | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter MP-1(a): *<Customer-defined personnel or roles>* | |
| Parameter MP-1(b)(1): *<FedRAMP Assignment: at least annually>* | |
| Parameter MP-1(b)(2): *<FedRAMP Assignment: at least annually or whenever a significant change occurs>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| MP-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for developing, documenting, reviewing, updating, and disseminating media protection policy and procedures. Due to there not being any customer-controlled media within the scope of systems deployed on Azure, all media protection controls will be implemented and managed by Azure. However, the customer is still responsible for the appropriate policy and procedure documents. The customer control implementation statement should address the frequency of review, the role(s) responsible, and the fact that there is no customer-controlled media within the scope of Azure and therefore the customer can inherit media protection controls from Azure. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for developing, documenting, reviewing, updating, and disseminating media protection policy and procedures. Due to there not being any customer-controlled media within the scope of systems deployed on Azure, all media protection controls will be implemented and managed by Azure. However, the customer is still responsible for the appropriate policy and procedure documents. The customer control implementation statement should address the frequency of review, the role(s) responsible, and the fact that there is no customer-controlled media within the scope of Azure and therefore the customer can inherit media protection controls from Azure. |

### MP-2 Media Access (H)

The organization restricts access to [FedRAMP Assignment: any digital and non-digital media deemed sensitive] to [Assignment: organization-defined personnel or roles].

| MP-2 | Control Summary Information |
| --- | --- |
| Responsible Role: Microsoft Azure | |
| Parameter MP-2-1: All media | |
| Parameter MP-2-2: Individuals who have a legitimate business purpose for accessing the data | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| MP-2 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure has implemented media access through the implementation of the Microsoft Security Policy. Logical access to digital media is controlled via Active Directory Group Policy Objects (AD GPOs) and security groups. Physical access to all media is restricted by the datacenter access process. Access is restricted to individuals who have a legitimate business purpose for accessing the data. Please refer to PE-3, Physical Access Control, for more details on the datacenter access controls in place. The Asset Protection Standard defines the safeguards required to protect the confidentiality, integrity, and availability of information assets within Microsoft Azure datacenters.  **Customer Responsibility (IaaS/PaaS)**  There is no customer-controlled media within the scope of systems deployed on Azure; all media protection controls are implemented and managed by Microsoft. This control is inherited from Azure. |

### 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: Microsoft Azure | |
| Parameter MP-3(b)-1: No removable media types | |
| Parameter MP-3(b)-2: 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| MP-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure marks assets within Microsoft datacenters with an HBI, MBI, or LBI (High, Moderate, or Low Business Impact) designation which requires different levels of security and handling precautions. Asset owners are required to classify their assets that are stored within a Microsoft datacenter. Refer to Asset Classification Standard and Asset Protection Standard for more information.  **Customer Responsibility (IaaS/PaaS)**  There is no customer-controlled media within the scope of systems deployed on Azure; all media protection controls are implemented and managed by Microsoft. This control is inherited from Azure. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure requires asset owners to assign their assets with an asset classification and no assets are exempt from this requirement. In the Microsoft datacenter environment, assets refer to servers, network devices, and magnetic tapes. Other digital media like USB flash/thumb drives, external/removable hard drives, or CD/DVDs are not used. Non-digital media is not used in the datacenter.  **Customer Responsibility (IaaS/PaaS)**  There is no customer-controlled media within the scope of systems deployed on Azure; all media protection controls are implemented and managed by Microsoft. This control is inherited from Azure. |

### 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: Microsoft Azure | |
| Parameter MP-4(a)-1: Digital media includes servers, network devices, and magnetic tapes used for backup. Non-digital media is not used in the datacenter environment. | |
| Parameter MP-4(a)-2: In the production datacenter 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| MP-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure digital media assets are physically and securely stored within datacenter colocation rooms. Microsoft datacenters have multiple layers of physical access controls (access badge, biometrics – see PE-3 for further details on physical access controls) and video surveillance in place to provide secure storage. Digital media for includes servers, network devices, and magnetic tapes used for backup. Non-digital media is not used in the datacenter environment.  **Customer Responsibility (IaaS/PaaS)**  There is no customer-controlled media within the scope of systems deployed on Azure; all media protection controls are implemented and managed by Microsoft. This control is inherited from Azure. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure digital media assets are protected in Microsoft datacenter colocations through physical access controls (PE-3) and logical access controls (IA-2) for the lifetime of the asset. Microsoft Azure assets are cleared, purged, or destroyed with methods consistent with NIST SP 800-88 prior to the assets disposal. For asset destruction, Microsoft Azure utilizes onsite asset destruction services.  **Customer Responsibility (IaaS/PaaS)**  There is no customer-controlled media within the scope of systems deployed on Azure; all media protection controls are implemented and managed by Microsoft. This control is inherited from Azure. |

### 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;
2. Documents activities associated with the transport of information system media; and
3. Restricts the activities associated with transport of information system media to authorized personnel.

| MP-5 | Control Summary Information |
| --- | --- |
| Responsible Role: Microsoft Azure | |
| Parameter MP-5(a)-1: Magnetic tapes, external/removable hard drives, diskettes, compact disks and digital video disks and non-digital media. | |
| Parameter MP-5(a)-2: Security functions are listed in Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| MP-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  Digital media at Microsoft datacenters consist of servers, network devices, and magnetic backup tapes and discs, where appropriate. Microsoft datacenters do not use non-digital media. Microsoft utilizes three methods to protect media that is being transported outside the datacenter: 1) Secure Transport, 2) Encryption 3) Cleanse, Purge, or Destroy.  **Customer Responsibility (IaaS/PaaS)**  There is no customer-controlled media within the scope of systems deployed on Azure; all media protection controls are implemented and managed by Microsoft. This control is inherited from Azure. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure maintains accountability for assets leaving the datacenter through the use of guidance from NIST SP 800-88: consistent cleansing/purging, asset destruction, encryption, accurate inventorying, tracking, and protection of chain of custody during transport.  **Customer Responsibility (IaaS/PaaS)**  There is no customer-controlled media within the scope of systems deployed on Azure; all media protection controls are implemented and managed by Microsoft. This control is inherited from Azure. |
| Part c | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure maintains records of inventory prior to transport, tracking and protection of chain of custody during transport, asset cleaning/purging, asset destruction, receipt of assets, and inventory validation after transport.  **Customer Responsibility (IaaS/PaaS)**  There is no customer-controlled media within the scope of systems deployed on Azure; all media protection controls are implemented and managed by Microsoft. This control is inherited from Azure. |
| Part d | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure restricts the activities of asset transport to authorized personnel through the protection of the chain of custody. The use of locks, tamper proof seals, and requiring validation of the asset inventories ensures that only authorized personnel are involved in the asset transport.  **Customer Responsibility (IaaS/PaaS)**  There is no customer-controlled media within the scope of systems deployed on Azure; all media protection controls are implemented and managed by Microsoft. This control is inherited from Azure. |

#### 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-5 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| MP-5 (4) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure employs Data Protection Service (DPS) to manage cryptographic keys using a FIPS 140-2 Level 3-validated encryption module (cert #1694) and HSM (cert #1178) to secure AES 256-bit encrypted data on the magnetic tapes.  **Customer Responsibility (IaaS/PaaS)**  There is no customer-controlled media within the scope of systems deployed on Azure; all media protection controls are implemented and managed by Microsoft. This control is inherited from Azure. |

### MP-6 Media Sanitization and Disposal (H)

The organization:

1. Sanitizes [Assignment: organization-defined information system media] prior to disposal, release out of organizational control, or release for reuse using [FedRAMP Assignment: techniques and procedures IAW NIST SP 800-88 and Section 5.9: Reuse and Disposal of Storage Media and Hardware] 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: Microsoft Azure | |
| Parameter MP-6(a)-1: All digital media | |
| Parameter MP-6(a)-2: Digital media: Overwrite at least 3 times; Non-digital media is not used by Microsoft Azure in the datacenter 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| MP-6 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure requires digital media in the Microsoft Azure datacenter environment to be cleansed/purged using Microsoft Azure approved tools and in a manner consistent with NIST SP 800-88, Guidelines for Media Sanitization, prior to being reused or disposed of. Non-digital media is not used by Microsoft Azure in the datacenter environment.  **Customer Responsibility (IaaS/PaaS)**  There is no customer-controlled media within the scope of systems deployed on Azure; all media protection controls are implemented and managed by Microsoft. This control is inherited from Azure. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure uses data erasure units and processes to cleanse/purge data in a manner consistent with NIST SP 800-88 and which are commensurate with the Microsoft Azure asset classification of the asset. For assets requiring destruction, Microsoft Azure utilizes onsite asset destruction services.  **Customer Responsibility (IaaS/PaaS)**  There is no customer-controlled media within the scope of systems deployed on Azure; all media protection controls are implemented and managed by Microsoft. This control is inherited from Azure. |

#### MP-6 (1) Control Enhancement (H)

The organization reviews, approves, tracks, documents, and verifies media sanitization and disposal actions.

| MP-6 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| MP-6 (1) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Azure has implemented media sanitization procedures in accordance with the guidance in NIST SP 800-88 for the Asset Classification Standard and Asset Protection Standard. All magnetic or electronic media is cleansed/purged by following NIST SP 800-88 specifications in accordance with its Azure asset classification. Azure utilizes data erasure units from Extreme Protocol Solutions (EPS). EPS software supports NIST SP 800-88 requirements for cleansing and purging/secure erasure.  **Customer Responsibility (IaaS/PaaS)**  There is no customer-controlled media within the scope of systems deployed on Azure; all media protection controls are implemented and managed by Microsoft. This control is inherited from Azure. |

#### MP-6 (2) Control Enhancement (H)

The organization tests sanitization equipment and procedures [FedRAMP Assignment: at least every six (6) months] 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-6 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: Microsoft Azure | |
| Parameter MP-6(2): every 180 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| MP-6 (2) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure uses data erasure units and processes to cleanse/purge data in a manner consistent with NIST SP 800-88. Every 180 days, DCS operations tests the Microsoft Azure data erasure units and the process for erasure. In the test, DCS operations verifies that the intended sanitization is being achieved through a forensic analysis of tested hard drives to confirm that the data has been sanitized by the data erasure units.  **Customer Responsibility (IaaS/PaaS)**  There is no customer-controlled media within the scope of systems deployed on Azure; all media protection controls are implemented and managed by Microsoft. This control is inherited from Azure. |

#### MP-6 (3) Control Enhancement (H)

The organization applies nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the information system under the following circumstances: [Assignment: organization-defined circumstances requiring sanitization of portable storage devices].

| MP-6 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: Microsoft Azure | |
| Parameter MP-6 (3): before use in the 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| MP-6 (3) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure ensures that Azure datacenters follow the Tools and Removable Media Security Procedure in the Data Center Services Run Book in order to prevent the infection of the Government environment by malware on portable storage devices. The procedure specifies that the following actions be taken with USB drives before use in the Government environment:  (1) Format the USB drives when the drives are first purchased from the manufacturer or vendor, before the initial use or when being reused for a different tool.  (2) Scan any USB drive to be used in a Government-designated area for malware, before taking the drive into the area.  (3) After using a drive within a Government-designated area, format the drive before leaving the area.  The Tools and Removable Media Security Procedure also requires that all lost, discarded, stolen or misplaced thumb drives never be re-introduced into Azure datacenters but that they be instead cataloged and destroyed.  **Customer Responsibility (IaaS/PaaS)**  There is no customer-controlled media within the scope of systems deployed on Azure; all media protection controls are implemented and managed by Microsoft. This control is inherited from Azure. |

### 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-7 | Control Summary Information |
| --- | --- |
| Responsible Role: Microsoft Azure | |
| Parameter MP-7-1: Prohibits | |
| Parameter MP-7-2: Defined information system media | |
| Parameter MP-7-3: All information systems | |
| Parameter MP-7-4: 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| MP-7 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure requires asset owners to assign their assets with an asset classification, and no assets are exempt from this requirement. In the Microsoft Azure datacenter environment, assets refer to servers, and network devices. Other digital media like USB flash/thumb drives are managed by specific policies and procedures governing how those devices are managed. CD/DVDs are not used. Non-digital media is not used in the datacenter. The usage of digital media in Microsoft Azure datacenter environments is monitored 24x7 via CCTV coverage.  Please see PE-06 for more details.  **Customer Responsibility (IaaS/PaaS)**  There is no customer-controlled media within the scope of systems deployed on Azure; all media protection controls are implemented and managed by Microsoft. This control is inherited from Azure. |

#### 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-7 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| MP-7 (1) is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft restricts the use of writable, removable media to media that has been explicitly approved by Datacenter Management via the DCS Tools and Removable Media Procedure. Media that is personally owned or has no identifiable owner is prohibited in any production area as noted in the Microsoft Datacenter Work Rules and Regulations document.  **Customer Responsibility (IaaS/PaaS)**  There is no customer-controlled media within the scope of systems deployed on Azure; all media protection controls are implemented and managed by Microsoft. This control is inherited from Azure. |

## Physical and Environmental Protection (PE)

### PE-1 Physical and Environmental Protection Policy and Procedures (H)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A physical and environmental 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 physical and environmental protection policy and associated physical and environmental protection controls; and
2. Reviews and updates the current:
   1. Physical and environmental protection policy [FedRAMP Assignment: at least annually]; and
   2. Physical and environmental protection procedures [FedRAMP Assignment: at least annually or whenever a significant change occurs].

| PE-1 | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter PE-1(a): *<Customer-defined personnel or roles>* | |
| Parameter PE-1(b)(1): *<*FedRAMP Assignment: at least annually> | |
| Parameter PE-1(b)(2): <FedRAMP Assignment: at least annually or whenever a significant change occurs> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| PE-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for developing, documenting, reviewing, updating, and disseminating physical and environmental protection policy and procedures. Due to customers not having physical access to any resources in Azure datacenters, all physical and environmental protection controls will be implemented and managed by Azure. However, the customer is still responsible for the appropriate policy and procedure documents. The customer control implementation statement should address the frequency of review, the role(s) responsible, and the fact that the customer does not have physical access to any Azure resources and therefore the customer can inherit physical and environmental controls from Azure. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for developing, documenting, reviewing, updating, and disseminating physical and environmental protection policy and procedures. Due to customers not having physical access to any resources in Azure datacenters, all physical and environmental protection controls will be implemented and managed by Azure. However, the customer is still responsible for the appropriate policy and procedure documents. The customer control implementation statement should address the frequency of review, the role(s) responsible, and the fact that the customer does not have physical access to any Azure resources and therefore the customer can inherit physical and environmental controls from Azure. |

### PE-2 Physical Access Authorizations (H)

The organization:

1. Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides;
2. Issues authorization credentials for facility access;
3. Reviews the access list detailing authorized facility access by individuals [FedRAMP Assignment: at least every ninety (90) days]; and
4. Removes individuals from the facility access list when access is no longer required.

| PE-2 | Control Summary Information |
| --- | --- |
| Responsible Role: Microsoft Azure | |
| Parameter PE-2(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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| PE-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure implements this requirement on behalf of customers. Physical access to a Microsoft datacenter must be approved by the Datacenter Management (DCM) team using the datacenter access tool. Access assignments require an end date, after which access is automatically removed and must be reapproved. Additionally, when access is no longer required, datacenter security officers or management to manually request the termination of access.  **Customer Responsibility (IaaS/PaaS)**  Customers do not have physical access to any system resources in Azure datacenters; all physical and environmental protection controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure implements this requirement on behalf of customers. The datacenter access tool is the authoritative source listing all personnel with authorized access to a specific datacenter. The tool is linked with the datacenter’s physical security access control devices and authorizes access based on access levels that are approved by the DCM team. Access levels are assigned in the tool to either a user’s Microsoft issued badge or a temporary access badge that is assigned at the datacenter by the Control Room Supervisor (CRS). Access levels are approved by the DCM team. In addition to credentials assigned to physical badges, some areas of the datacenter require enrollment of the user’s biometric data (hand geometry or fingerprint).  **Customer Responsibility (IaaS/PaaS)**  Customers do not have physical access to any system resources in Azure datacenters; all physical and environmental protection controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure. |
| Part c | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure implements this requirement on behalf of customers. In addition to the access revocation described in part a, Microsoft Azure reviews authorized access lists for Azure datacenters every 90 days in order to remove/update individual access as necessary.  **Customer Responsibility (IaaS/PaaS)**  Customers do not have physical access to any system resources in Azure datacenters; all physical and environmental protection controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure. |
| Part d | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure implements this requirement on behalf of customers. Microsoft Azure removes access automatically when the access assignment end date is reached. When access is no longer required, datacenter security officers or management will manually request the termination of access in the datacenter access tool. Additionally, Microsoft Azure will remove any unneeded access authorizations discovered as a result of the access list review described in part c.  **Customer Responsibility (IaaS/PaaS)**  Customers do not have physical access to any system resources in Azure datacenters; all physical and environmental protection controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure. |

### 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:
   1. Verifying individual access authorizations before granting access to the facility; and
   2. Controlling ingress/egress to the facility using [FedRAMP Assignment: CSP defined physical access control systems/devices AND guards];
2. Maintains physical access audit logs for [Assignment: organization-defined entry/exit points];
3. Provides [Assignment: organization-defined security safeguards] to control access to areas within the facility officially designated as publicly accessible;
4. Escorts visitors and monitors visitor activity [FedRAMP Assignment: in all circumstances within restricted access area where the information system resides];
5. Secures keys, combinations, and other physical access devices;
6. Inventories [Assignment: organization-defined physical access devices] every [FedRAMP Assignment: at least annually]; and
7. 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: Microsoft Azure | |
| Parameter PE-3(a): All physical access points to the facility | |
| Parameter PE-3(a)(2): Defined physical access control systems/devices | |
| Parameter PE-3(b): All physical access points to the facility | |
| Parameter PE-3(c): Guards during working hours; guards, locks, and/or alarms during non-working hours | |
| Parameter PE-3(d): At all times while in the datacenter | |
| Parameter PE-3(f)-1: Keys, temporary access badges, access badge readers, and similar devices | |
| Parameter PE-3(f)-2: Annually | |
| Parameter PE-3(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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| PE-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure implements this requirement on behalf of customers. Microsoft Azure enforces physical access authorizations for all physical access points to Azure datacenters using 24x7 staffing, alarms, video surveillance, multifactor authentication, and man-trap portal devices.  **Customer Responsibility (IaaS/PaaS)**  Customers do not have physical access to any system resources in Azure datacenters; all physical and environmental protection controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure implements this requirement on behalf of customers. All accesses to Azure datacenter facilities are logged and audited.  **Customer Responsibility (IaaS/PaaS)**  Customers do not have physical access to any system resources in Azure datacenters; all physical and environmental protection controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure. |
| Part c | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure implements this requirement on behalf of customers. Azure datacenters do not contain areas that are designated as publicly accessible.  **Customer Responsibility (IaaS/PaaS)**  Customers do not have physical access to any system resources in Azure datacenters; all physical and environmental protection controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure. |
| Part d | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure implements this requirement on behalf of customers. All visitors that have approved access to the datacenter (See PE-2) are designated as “Escort Only” on their badges or through other visual cue (e.g., colored badges) and are required to remain with their escorts at all times. Escorted visitors do not have any access levels granted to them and can only travel on the access of their escorts. Escorts monitor all activities of their visitor while in the datacenter.  **Customer Responsibility (IaaS/PaaS)**  Customers do not have physical access to any system resources in Azure datacenters; all physical and environmental protection controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure. |
| Part e | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure implements this requirement on behalf of customers. Physical keys and temporary access badges are secured within the security operations center (SOC). Security officers are staffed 24x7. Keys are checked out to specific personnel by matching the person’s access badge to the physical key. Key inventories are conducted during each shift and keys are not allowed to be taken offsite.  **Customer Responsibility (IaaS/PaaS)**  Customers do not have physical access to any system resources in Azure datacenters; all physical and environmental protection controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure. |
| Part f | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure implements this requirement on behalf of customers. Physical access devices within Azure datacenters are inventoried on at least an annual basis. Keys and temporary access badges are inventoried multiple times a day during each shift. Access badge readers and similar access devices are linked to the physical security system where status is continuously represented.  **Customer Responsibility (IaaS/PaaS)**  Customers do not have physical access to any system resources in Azure datacenters; all physical and environmental protection controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure. |
| Part g | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure implements this requirement on behalf of customers. Microsoft Azure datacenters have procedures to implement in cases when an access badge or key is lost or a person is terminated or transferred. In the event of a termination or transfer, the person’s access is immediately removed from the system and their access badge removed.  **Customer Responsibility (IaaS/PaaS)**  Customers do not have physical access to any system resources in Azure datacenters; all physical and environmental protection controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure. |

#### PE-3 (1) Control Enhancement (H)

The organization enforces physical access authorizations to the information system in addition to the physical access controls for the facility at [Assignment: organization-defined physical spaces containing components of the information system].

| PE-3 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Microsoft Azure | |
| Parameter PE-3 (1): Areas within Microsoft datacenters that contain critical systems (e.g., colocations, critical environments, MDF rooms, etc.) | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| PE-3 (1) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure further restricts areas within Microsoft datacenters that contain critical systems (e.g., colocations, critical environments, MDF rooms, etc.) through various security mechanisms such as electronic access control, biometric devices, and anti-passback controls. Access to Azure colocations are granted as a separate, higher level of DCAT access than other access areas of the datacenter. In addition, all Azure FTE's and vendors who have access to the Azure Government colocations are required to formally undergo Microsoft's Cloud Screening and US citizenship verification prior to being authorized access to the environment. See PS-03 section for further details regarding the cloud screening for the Azure Government colocations.  **Customer Responsibility (IaaS/PaaS)**  Customers do not have physical access to any system resources in Azure datacenters; all physical and environmental protection controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure. |

### 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-4 | Control Summary Information |
| --- | --- |
| Responsible Role: Microsoft Azure | |
| Parameter PE-4-1: All distribution and transmission lines | |
| Parameter PE-4-2: 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| PE-4 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure implements this requirement on behalf of customers. Microsoft Azure has implemented access control for transmission medium through the design and building of the Main Distribution Frame (MDF) rooms and colocations to protect information system distribution and transmission lines from accidental damage, disruption, and physical tampering. Access to MDF rooms and colocations require two factor authentication (access badge and biometrics). This ensures that access is restricted to only authorized personnel (See PE-2, PE-3). Within the MDF, transmission and distribution lines are protected from accidental damage, disruption, and physical tampering through the use of metal conduits, locked racks, cages, or cable trays.  **Customer Responsibility (IaaS/PaaS)**  Customers do not have physical access to any system resources in Azure datacenters; all physical and environmental protection controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure. |

### 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-5 | Control Summary Information |
| --- | --- |
| Responsible Role: Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| PE-5 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure implements this requirement on behalf of customers. Microsoft Azure datacenters do not have output devices (monitors, printers, audio devices, etc.) permanently connected to Azure assets or Azure shared assets. In addition to not having output devices, security officers perform physical walkthroughs of the facility multiple times per shift checking for items like doors being locked and racks being secured. Datacenter access is limited to people who have approved access authorizations. Colocations require two factor authentication (access badge and biometrics) to gain access.  **Customer Responsibility (IaaS/PaaS)**  Customers do not have physical access to any system resources in Azure datacenters; all physical and environmental protection controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure. |

### 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: Microsoft Azure | |
| Parameter PE-6(b)-1: Continuously | |
| Parameter PE-6(b)-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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| PE-6 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure implements this requirement on behalf of customers. Physical access is monitored by implementing security devices and processes at the datacenters. Examples include 24x7 electronic monitoring of access control, alarm and video systems as well as 24x7 on site security patrols of the facility and grounds. A Control Room Supervisor is located in the SOC at all times to provide monitoring of physical access in the datacenter.  **Customer Responsibility (IaaS/PaaS)**  Customers do not have physical access to any system resources in Azure datacenters; all physical and environmental protection controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure implements this requirement on behalf of customers. Physical access logs are reviewed continuously, and maintained for subsequent investigative review.  **Customer Responsibility (IaaS/PaaS)**  Customers do not have physical access to any system resources in Azure datacenters; all physical and environmental protection controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure. |
| Part c | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure implements this requirement on behalf of customers. Security events that occur within the datacenter are documented by the security team. The security team creates reports that capture the details of a security event after the event occurs.  For incidents requiring government notification, the Microsoft Azure security team will coordinate with the major application provider (e.g., O365) to notify the government agency customer, US CERT, and FedRAMP within US-CERT guidelines (see IR-6).  **Customer Responsibility (IaaS/PaaS)**  Customers do not have physical access to any system resources in Azure datacenters; all physical and environmental protection controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure. |

#### PE-6 (1) Control Enhancement (M) (H)

The organization monitors physical intrusion alarms and surveillance equipment.

| PE-6 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| PE-6 (1) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure implements this requirement on behalf of customers. In addition to the 24x7 onsite security, Microsoft Azure datacenters (leased and fully managed) also utilize alarm monitoring systems and CCTV. Alarms are monitored and responded to by the Control Room Supervisor stationed 24x7 in the SOC. During a response situation, the Control Room Supervisor utilizes cameras in the area of the incident being investigated to give the responder real-time information.  **Customer Responsibility (IaaS/PaaS)**  Customers do not have physical access to any system resources in Azure datacenters; all physical and environmental protection controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure. |

#### PE-6 (4) Control Enhancement (H)

The organization monitors physical access to the information system in addition to the physical access monitoring of the facility as [Assignment: organization-defined physical spaces containing one or more components of the information system].

| PE-6 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: Microsoft Azure | |
| Parameter PE-6 (4): perimeter doors, facility entrances and exits, interior aisles, caged areas, high-security areas, shipping and receiving, facility external areas such as parking lots and other areas of the facility | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| PE-6 (4) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure monitors physical access to the facilities as well as the information systems within the datacenters. All Microsoft’s online services’ equipment is placed in locations within datacenters where physical access is monitored. All of the colocation and MDF rooms are protected by access control, alarms, and video.  **Customer Responsibility (IaaS/PaaS)**  Customers do not have physical access to any system resources in Azure datacenters; all physical and environmental protection controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure. |

### 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: Microsoft Azure | |
| Parameter PE-8(a): At least one year | |
| Parameter PE-8(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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| PE-8 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure implements this requirement on behalf of customers. Datacenter access records are maintained in the datacenter access tool in the form of approved requests. As described in PE-3, visitors are required to be escorted at all times. The escort’s access within the datacenter is logged and if necessary can be correlated to the visitor for future review.  **Customer Responsibility (IaaS/PaaS)**  Customers do not have physical access to any system resources in Azure datacenters; all physical and environmental protection controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure implements this requirement on behalf of customers. Visitors with an approved access request will have their access record reviewed at the time their identification is verified against a form of government issued ID or Microsoft issued badge. As described in PE-3, visitors are escorted at all times while at the datacenter.  **Customer Responsibility (IaaS/PaaS)**  Customers do not have physical access to any system resources in Azure datacenters; all physical and environmental protection controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure. |

#### PE-8 (1) Control Enhancement (H)

The organization employs automated mechanisms to facilitate the maintenance and review of visitor access records.

| PE-8 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| PE-8 (1) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure maintains datacenter access records in DCAT in the form of approved DCAT requests. DCAT requests can only be approved by the DCM team. Access levels within the datacenter are assigned and managed within DCAT. Datacenter access is reviewed quarterly. All access to Azure datacenters is recorded in DCAT and is available for future possible investigations. Visitors are required to be escorted at all times. The escort’s access within the datacenter is logged within the alarm monitoring system and if necessary can be correlated to the visitor for future review.  Visitor access is being reviewed continuously by the assigned escort and by the control room supervisor via CCTV and the alarm monitoring system.  Visitors are not provided with access and must be accompanied by their escorts at all times.  **Customer Responsibility (IaaS/PaaS)**  Customers do not have physical access to any system resources in Azure datacenters; all physical and environmental protection controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure. |

### 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: Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| PE-9 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure implements this requirement on behalf of customers. Microsoft Azure provides protective spaces and appropriate labeling for cables. Microsoft Azure infrastructure equipment—for example, cables, electrical lines, and backup generators—must be placed in environments which have been engineered to be protected from environmental risks such as theft, fire, explosives, smoke, water, dust, vibration, earthquake, harmful chemicals, electrical interference, power outages, electrical disturbances (spikes). All portable online services’ assets (e.g., racks, servers, network devices) must be locked or fastened in place in order to provide protection against theft or movement damage. Power and information system cables within any Microsoft Azure environment are labeled appropriately and protected against interception or damage. Power and information system cables are separated from each other at all points within an environment to avoid interference.  **Customer Responsibility (IaaS/PaaS)**  Customers do not have physical access to any system resources in Azure datacenters; all physical and environmental protection controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure. |

### 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: Microsoft Azure | |
| Parameter PE-10(b): Colocations or manned Facilities Operation Centers (FOCs) | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| PE-10 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure implements this requirement on behalf of customers. Microsoft Azure has installed Emergency Power Off (EPO) buttons in locations within the datacenter as required by local fire code. In some Microsoft Azure managed datacenters, the datacenter design no longer requires EPO buttons.  **Customer Responsibility (IaaS/PaaS)**  Customers do not have physical access to any system resources in Azure datacenters; all physical and environmental protection controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure implements this requirement on behalf of customers. EPO buttons are strategically placed to allow for activation in emergency situations. EPO buttons can be placed in the colocations, manned Facilities Operation Centers (FOCs), or as required by local fire code.  **Customer Responsibility (IaaS/PaaS)**  Customers do not have physical access to any system resources in Azure datacenters; all physical and environmental protection controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure. |
| Part c | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure implements this requirement on behalf of customers. To prevent accidental activation, EPO buttons may have a protective enclosure, require dual activation, or utilize an audible alarm as a warning before activation. Additionally, EPO buttons are under video surveillance.  **Customer Responsibility (IaaS/PaaS)**  Customers do not have physical access to any system resources in Azure datacenters; all physical and environmental protection controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure. |

### 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: Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| PE-11 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure implements this requirement on behalf of customers. Microsoft Azure has implemented emergency power by protecting datacenter equipment and circuits with an uninterruptible power supply (UPS) system which provides a short-term power supply to provide power until generators are able to come online.  **Customer Responsibility (IaaS/PaaS)**  Customers do not have physical access to any system resources in Azure datacenters; all physical and environmental protection controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure. |

#### PE-11 (1) Control Enhancement (H)

The organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.

| PE-11 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| PE-11 (1) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure has implemented a long-term alternate power supply for the information system that is capable of maintaining a minimum required operational capability when an extended loss of the primary power source occurs. When power fails or drops to an unacceptable voltage level, Uninterruptable Power Supply (UPS) systems instantly kick in and take over the power load. This provides enough power for running the servers until the generators can take over. Emergency generators provide back-up power for extended outages and for planned maintenance, and can operate the data center with on-site fuel reserves in the event of a natural disaster. Azure maintains diesel generator at many of our datacenters. Backup generators are used when necessary to help maintain grid stability or in extraordinary repair, and maintenance situations that require us to take our datacenters off the power grid.  **Customer Responsibility (IaaS/PaaS)**  Customers do not have physical access to any system resources in Azure datacenters; all physical and environmental protection controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure. |

### 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: Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| PE-12 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure implements this requirement on behalf of customers. Microsoft Azure datacenters (leased and fully managed) implement emergency lighting in the form of overhead emergency lighting on dedicated circuits backed up by UPS and generator systems (See PE-11). Automatic emergency lighting is implemented along all evacuation routes, emergency exits, and inside the colocations in accordance with the National Fire and Protection Association (NFPA) Life Safety Code. In the event that utility power is lost, the emergency lighting will automatically switch to power provided by the UPS and generator systems. The emergency lighting systems within Microsoft Azure datacenters undergo routine maintenance to ensure that they remain in proper working order.  **Customer Responsibility (IaaS/PaaS)**  Customers do not have physical access to any system resources in Azure datacenters; all physical and environmental protection controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure. |

### 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: Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| PE-13 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure implements this requirement on behalf of customers. Microsoft Azure has implemented fire protection by installing fire detection and fire suppression systems at the Microsoft Azure datacenters.  Microsoft Azure datacenters implement robust fire detection mechanisms. The Microsoft Azure fire protection approach includes the use of photoelectric smoke detectors installed below the floor and on the ceiling which are integrated with the fire protection sprinkler system. Additionally, there are Xtralis VESDA (Very Early Smoke Detection Apparatus) systems in each colocation which monitor the air. VESDA units are highly-sensitive air sampling systems installed throughout multiple high-value spaces. VESDA units allow for an investigative response prior to an actual fire detection alarm.  “Pull station” fire alarm boxes are installed throughout the datacenters for manual fire alarm notification. Fire extinguishers are located throughout the datacenters and are properly inspected, serviced, and tagged annually. The security staff patrols all building areas multiple times every shift. Datacenter personnel perform a daily site walk-through ensuring all fire watch requirements are being met.  Areas containing sensitive electrical equipment (colocations, MDFs, etc.) are protected by double interlock pre-action (dry pipe) sprinkler systems. Dry pipe sprinklers are a two-stage pre-action system that requires both a sprinkler head activation (due to heat) as well as smoke detection to release water. The sprinkler head activation releases the air pressure in the pipes which allows the pipes to fill with water. Water is released when a smoke or heat detector is also activated.  Fire detection/suppression and emergency lighting systems are wired into the datacenter UPS and generator systems providing for a redundant power source.  **Customer Responsibility (IaaS/PaaS)**  Customers do not have physical access to any system resources in Azure datacenters; all physical and environmental protection controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure. |

#### PE-13 (1) Control Enhancement (H)

The organization employs fire detection devices/systems for the information system that activate automatically and notify [FedRAMP Assignment: service provider building maintenance/physical security personnel] and [FedRAMP Assignment: service provider emergency responders with incident response responsibilities] in the event of a fire.

| PE-13 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Microsoft Azure | |
| Parameter PE-13 (1)-1: Local security staff and the Global Security Operations Center in Redmond | |
| Parameter PE-13 (1)-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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| PE-13 (1) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Azure employs fire detection devices/systems for the information system that activate automatically and notify datacenter personnel along with emergency responders in the event of a fire. In the event that one of the fire detection mechanisms is activated in any colocation, the local fire department is automatically notified through the fire alarm system. In addition, the fire protection and fire detection systems are tied into the security system notifying the local facility and security staff.  **Customer Responsibility (IaaS/PaaS)**  Customers do not have physical access to any system resources in Azure datacenters; all physical and environmental protection controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure. |

#### 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: Microsoft Azure | |
| Parameter PE-13(2)-1: Local security staff and the Global Security Operations Center in Redmond | |
| Parameter PE-13(2)-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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| PE-13 (2) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure implements this requirement on behalf of customers. In the event that one of the fire suppression systems is activated at the datacenter, the local fire department is automatically notified through the fire alarm system. In addition, the fire protection and fire detection systems are tied into the security system notifying the local facility and security staff.  **Customer Responsibility (IaaS/PaaS)**  Customers do not have physical access to any system resources in Azure datacenters; all physical and environmental protection controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure. |

#### 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: Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| PE-13 (3) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure implements this requirement on behalf of customers. Microsoft Azure datacenters are staffed 24x7. Fire suppression systems engage automatically without manual intervention when a fire alarm situation is detected.  **Customer Responsibility (IaaS/PaaS)**  Customers do not have physical access to any system resources in Azure datacenters; all physical and environmental protection controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure. |

### 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: Microsoft Azure | |
| Parameter PE-14(a): In accordance with ASHRAE guidelines | |
| Parameter PE-14(b): Continuously | |
| Parameter PE-14(b) Additional: Temperature range is 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%. | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| PE-14 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure implements this requirement on behalf of customers. Microsoft Azure maintains the temperature and humidity levels in accordance with American Society of Heating, Refrigerating and Air-conditioning Engineers (ASHRAE) guidelines. The temperature and humidity levels are monitored continuously by the datacenter’s Building Management System (BMS).  **Customer Responsibility (IaaS/PaaS)**  Customers do not have physical access to any system resources in Azure datacenters; all physical and environmental protection controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure implements this requirement on behalf of customers. At Microsoft Azure datacenters, temperature and humidity levels are monitored continuously by the Building Management System (BMS). Datacenter personnel monitor the BMS from the Facilities Operations Center (FOC), so that they can manage the temperature and humidity within the datacenter before any alarm points are exceeded.  **Customer Responsibility (IaaS/PaaS)**  Customers do not have physical access to any system resources in Azure datacenters; all physical and environmental protection controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure. |

#### 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: Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| PE-14 (2) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure implements this requirement on behalf of customers. At Microsoft Azure datacenters, temperature and humidity levels are monitored continuously by the Building Management System (BMS). Datacenter personnel monitor the BMS from the Facilities Operations Center (FOC), so that they can manage the temperature and humidity within the datacenter before any alarm points are exceeded.  **Customer Responsibility (IaaS/PaaS)**  Customers do not have physical access to any system resources in Azure datacenters; all physical and environmental protection controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure. |

### 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: Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| PE-15 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure implements this requirement on behalf of customers. Microsoft Azure provides water/leak detection in areas with a risk of water leakage (e.g., Air Handlers Units). Fire suppression systems also have leak detection alarms that are monitored. The water/leak detection system is integrated with the facility alarm and notification system. The sprinkler systems in the datacenters are zoned. Datacenter personnel are familiar with emergency procedures requiring the use of the water shutoff valves and their locations. The sprinkler risers have the ability to be shut off individually or as a group via gate valves. All sprinklers in the critical space are double interlock pre-action type sprinklers that require two forms of activation before flow is initiated. The pressure of the sprinkler system is monitored and alarmed against water leakage.  **Customer Responsibility (IaaS/PaaS)**  Customers do not have physical access to any system resources in Azure datacenters; all physical and environmental protection controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure. |

#### PE-15 (1) Control Enhancement (H)

The organization employs automated mechanisms to detect the presence of water in the vicinity of the information system and alerts [FedRAMP Assignment: service provider building maintenance /physical security personnel].

| PE-15 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Microsoft Azure | |
| Parameter PE-15 (1): Local security staff and the Global Security Operations Center in Redmond | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| PE-15 (1) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Azure employs automated mechanism to detect water presence in the datacenters and alerts datacenter personnel. Azure provides water/leak detection in areas with a risk of water leakage (e.g., Air Handlers Units). Fire suppression systems also have leak detection alarms that are monitored. The water/leak detection system is integrated with the facility alarm and notification system. The pressure of the sprinkler system is monitored and alarmed against water leakage.  **Customer Responsibility (IaaS/PaaS)**  Customers do not have physical access to any system resources in Azure datacenters; all physical and environmental protection controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure. |

### 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: Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| PE-16 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure implements this requirement on behalf of customers. Microsoft Azure implements strict enforcement of what is allowed to enter and exit the datacenter. All system components/assets are tracked in the asset management tool database.  **Customer Responsibility (IaaS/PaaS)**  Customers do not have physical access to any system resources in Azure datacenters; all physical and environmental protection controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure. |

### 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: Microsoft Azure | |
| Parameter PE-17(a): Appropriate management, operational, and technical controls are defined for alternate work sites. | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| PE-17 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure implements this requirement on behalf of customers. Microsoft owns multiple buildings from which Microsoft employees can work from in the case of an emergency in a particular building or set of buildings. Microsoft buildings are built and operated to the same security standards.  **Customer Responsibility (IaaS/PaaS)**  Customers do not have physical access to any system resources in Azure datacenters; all physical and environmental protection controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure implements this requirement on behalf of customers. Microsoft is responsible for assessing the security controls at all of the Microsoft buildings.  **Customer Responsibility (IaaS/PaaS)**  Customers do not have physical access to any system resources in Azure datacenters; all physical and environmental protection controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure. |
| Part c | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure implements this requirement on behalf of customers. Microsoft is responsible for providing a means for employees to communicate with information security personnel in case of security incidents or problems.  **Customer Responsibility (IaaS/PaaS)**  Customers do not have physical access to any system resources in Azure datacenters; all physical and environmental protection controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure. |

### PE-18 Location of Information System Components (H)

The organization positions information system components within the facility to minimize potential damage from [FedRAMP Assignment: physical and environmental hazards identified during threat assessment] and to minimize the opportunity for unauthorized access.

| PE-18 | Control Summary Information |
| --- | --- |
| Responsible Role: Microsoft Azure | |
| Parameter PE-18: Environmental risks such as theft, fire, explosives, smoke, water, dust, vibration, earthquake, harmful chemicals, electrical interference, power outages, electrical disturbances (spikes), and radiation. | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| PE-18 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Azure implements strategic datacenter design approach to satisfy the location of information system components control. All Microsoft’s online services’ equipment is placed in locations which have been engineered to be protected from environmental risks such as theft, fire, explosives, smoke, water, dust, vibration, earthquake, harmful chemicals, electrical interference, power outages, electrical disturbances (spikes), and radiation. The facility and infrastructure have implemented seismic bracing for protection against environmental hazards. All of the colocation and MDF rooms are protected by access control, alarms, and video. The facility is also patrolled by security officers 24x7. All portable Azure assets are locked or fastened in place in order to provide protection against theft or movement damage.  **Customer Responsibility (IaaS/PaaS)**  Customers do not have physical access to any system resources in Azure datacenters; all physical and environmental protection controls are implemented and managed by Microsoft Azure. This control is inherited from Microsoft Azure. |

## Planning (PL)

### PL-1 Security Planning Policy and Procedures (H)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A security planning 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 planning policy and associated security planning controls; and
2. Reviews and updates the current:
   1. Security planning policy [FedRAMP Assignment: at least annually]; and
   2. Security planning procedures [FedRAMP Assignment: at least annually or whenever a significant change occurs].

| PL-1 | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter PL-1(a): *<Customer-defined personnel or roles>* | |
| Parameter PL-1(b)(1): *<FedRAMP Assignment: at least annually>* | |
| Parameter PL-1(b)(2): *<FedRAMP Assignment: at least annually or whenever a significant change occurs>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| PL-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for developing, documenting, reviewing, updating, and disseminating planning policy and procedures for customer-deployed resources. The customer control implementation statement should address the content of the policy (which must include purpose, scope, roles, responsibilities, management commitment, coordination, and compliance), procedures (which must facilitate the implementation of the policies and associated controls), the frequency of review, and the role(s) responsible. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for developing, documenting, reviewing, updating, and disseminating planning policy and procedures for customer-deployed resources. The customer control implementation statement should address the content of the policy (which must include purpose, scope, roles, responsibilities, management commitment, coordination, and compliance), procedures (which must facilitate the implementation of the policies and associated controls), the frequency of review, and the role(s) responsible. |

### 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: *<Customer-defined>* | |
| Parameter PL-2(b): *<Customer-defined personnel or roles>* | |
| Parameter PL-2(c): *<*FedRAMP Assignment: 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| PL-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for developing a system security plan (SSP) that meets the criteria defined by the target authorization (e.g., FedRAMP). Customers may reference NIST Special Publication 800-18 R1, Guide for Developing Security Plans for Federal Information Systems. The customer SSP should address controls inherited from Microsoft Azure and refer to the Microsoft Azure SSP for implementation details. The customer control implementation statement should address how the SSP is developed, distributed, reviewed updated, and protected. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for distributing the system security plan. The customer control implementation statement should address the key personnel (identified by name and/or role) and customer elements who should receive a copy of the system security plan defined in PL-02.a. |
| Part c | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for reviewing the system security plan. The customer control implementation statement should address the frequency with which the system security plan is reviewed. |
| Part d | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for updating the system security plan. The customer control implementation statement should address how updates reflect changes to the resources or environment of operation; and the problems encountered during plan implementation or security control assessments. |
| Part e | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for protecting the system security plan. The customer control implementation statement should address the process for preventing unauthorized disclosure or modification of the plan. |

#### 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-2 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter PL-2(3): *<Customer-defined individuals or groups>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| PL-2 (3) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for planning and coordinating security-related activities to reduce the impact on other organizational entities. The customer control implementation statement should address the customer-defined individuals or groups included in security-related activities (e.g., security assessments, audits, maintenance, patch management, and contingency plan testing). |

### PL-4 Rules of Behavior (H)

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;
2. 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;
3. Reviews and updates the rules of behavior [FedRAMP Assignment: annually]; and
4. 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: *<Customer-defined>* | |
| Parameter PL-4(c): *<FedRAMP Assignment: 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| PL-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for establishing rules of behavior. The customer control implementation statement should address the process of making the rules readily available to individuals requiring access to customer-deployed resources, and should describe their responsibilities and expected behavior when accessing such resources. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for obtaining signed acknowledgment of the rules of behavior from system users. The customer control implementation statement should address the process for withholding authorization until signatures are obtained. |
| Part c | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for reviewing and updating the rules of behavior. The customer control implementation statement should address the frequency with which the rules of behavior are reviewed and updated. |
| Part d | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for obtaining signed acknowledgment of the updated rules of behavior from system users. The customer control implementation statement should address the process for requiring users to read and re-sign when the rules of behavior are revised/updated. |

#### 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-4 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| PL-4 (1) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for including restrictions on the use of social media/networking sites and posting organizational information on public websites in the rules of behavior. The customer control implementation statement should address the explicit restrictions to be included in the rules of behavior. |

### PL-8 Information Security Architecture (M) (H)

The organization:

1. Develops an information security architecture for the information system that:
   1. Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information;
   2. Describes how the information security architecture is integrated into and supports the enterprise architecture; and
   3. Describes any information security assumptions about, and dependencies on, external services;
2. 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: *<Customer-defined>* | |
| Parameter PL-8(b): *<F*edRAMP Assignment: at least annually or when a significant change occurs> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| PL-8 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for developing an information security architecture for customer-deployed resources. The customer control implementation statement should address how the architecture describes: the overall philosophy, requirements, and approach to be taken with regard to protecting the CIA of information; how the information security architecture is integrated into and supports the enterprise architecture; and any information security assumptions about, and dependencies on, external services. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for reviewing and updating the information security architecture. The customer control implementation statement should address the frequency with which the information security architecture is reviewed and updated to reflect enterprise architecture updates. |
| Part c | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for accounting for planned changes to the information security architecture. The customer control implementation statement should address how these changes are reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurements/acquisitions. |

## Personnel Security (PS)

### PS-1 Personnel Security Policy and Procedures (H)

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 annually]; and
   2. Personnel security procedures [FedRAMP Assignment: at least annually or whenever a significant change occurs].

| PS-1 | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter PS-1(a): *<Customer-defined personnel or roles>* | |
| Parameter PS-1(b)(1): <FedRAMP Assignment: at least annually> | |
| Parameter PS-1(b)(2): <FedRAMP Assignment: 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) | |

| PS-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for developing, documenting, reviewing, updating, and disseminating personnel security policy and procedures for the personnel associated with the customer-deployed system. The customer control implementation statement should address the content of the policy (which must include purpose, scope, roles, responsibilities, management commitment, coordination, and compliance), procedures (which must facilitate the implementation of the policies and associated controls), the frequency of review, and the role(s) responsible. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for developing, documenting, reviewing, updating, and disseminating personnel security policy and procedures for the personnel associated with the customer-deployed system. The customer control implementation statement should address the content of the policy (which must include purpose, scope, roles, responsibilities, management commitment, coordination, and compliance), procedures (which must facilitate the implementation of the policies and associated controls), the frequency of review, and the role(s) responsible. |

### PS-2 Position Categorization (H)

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 annually].

| PS-2 | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter PS-2(c): <FedRAMP Assignment: 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| PS-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for assigning a risk designation. The customer control implementation statement should address the criteria used in risk designation assignments (e.g., specific responsibilities, access to certain types of data). |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for establishing screening criteria. The customer control implementation statement should address the criteria used to screen individuals filling the positions identified in PS-02.a. |
| Part c | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for reviewing and updating risk designations. The customer control implementation statement should address the frequency with which position risk designations are reviewed and updated. |

### 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: *<Customer-defined>* | |
| Parameter PS-3(b): <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> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| PS-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for screening individuals prior to authorizing access to customer-deployed resources. The customer control implementation statement should address how the screening requirements defined in PS-02 occur prior to authorizing access. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for rescreening individuals. The customer control implementation statement should address the customer-defined frequency and conditions under which rescreening will occur. |

#### 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: *<Customer-defined>* | |
| Parameter PS-3 (3)(b): <FedRAMP Assignment: personnel screening criteria – as required by specific 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| PS-3 (3) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for controlling access to protected information. The customer control implementation statement should address the requirement that individuals accessing customer-deployed resources which process, store, or transmit information requiring special protection have been assigned official government duties that demonstrate valid access authorizations. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for controlling access to protected information. The customer control implementation statement should address the requirement that individuals accessing customer-deployed resources which process, store, or transmit information requiring special protection satisfy any additional customer-defined personnel screening criteria. |

### PS-4 Personnel Termination (H)

The organization, upon termination of individual employment:

1. Disables information system access within [FedRAMP Assignment: eight (8) hours];
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: *<Customer-defined>* | |
| Parameter PS-4(a): <FedRAMP Assignment: eight (8) hours> | |
| Parameter PS-4(c): *<Customer-defined* information security topics> | |
| Parameter PS-4(f)-1: *<Customer-defined personnel or roles>* | |
| Parameter PS-4(f)-2: *<Customer-defined time period>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| PS-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for appropriately terminating customer personnel. The customer control implementation statement should address the time period within which system access must be disabled after termination. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for appropriately terminating customer personnel. The customer control implementation statement should address the termination/revocation of any authenticators/credentials associated with terminated individuals. |
| Part c | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for appropriately terminating customer personnel. The customer control implementation statement should address the requirement to conduct exit interviews which include customer-defined information security topics upon termination. |
| Part d | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for appropriately terminating customer personnel. The customer control implementation statement should address the retrieval of all security- and system-related property upon termination. |
| Part e | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for appropriately terminating customer personnel. The customer control implementation statement should address the requirement that the customer retains access to resources formally controlled by terminated individuals. |
| Part f | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for appropriately terminating customer personnel. The customer control implementation statement should address the requirement that customer-defined personnel/roles are notified of terminations within a customer-defined time period. |

#### PS-4 (2) Control Enhancement (H)

The organization employs automated mechanisms to notify [FedRAMP Assignment: access control personnel responsible for disabling access to the system] upon termination of an individual.

| PS-4 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter PS-4 (2): <FedRAMP Assignment: access control personnel responsible for disabling access to the system> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| PS-4 (2) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for employing automated mechanisms to notify the appropriate personnel upon termination of a customer employee. The customer control implementation statement should address the mechanisms used when customer personnel are terminated, and the customer-defined personnel/roles to be notified. |

### PS-5 Personnel Transfer (H)

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 [FedRAMP Assignment: twenty-four (24) hours];
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: twenty-four (24) hours].

| PS-5 | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter PS-5(b)-1: *<Customer-defined transfer or reassignment actions>* | |
| Parameter PS-5(b)-2: *<*FedRAMP Assignment: twenty-four (24) hours> | |
| Parameter PS-5(d)-1: *<Customer-defined personnel or roles>* | |
| Parameter PS-5(d)-2: *<FedRAMP Assignment: twenty-four (24) hours>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| PS-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for appropriately transferring personnel. The customer control implementation statement should address the review of current logical and physical access authorizations to customer-deployed resources/facilities when individuals are reassigned or transferred. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for appropriately transferring personnel. The customer control implementation statement should address the time period following formal transfer/reassignment within which customer-defined actions must be taken. |
| Part c | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for appropriately transferring personnel. The customer control implementation statement should address the modification of access authorizations as needed as a result of the review performed in PS-05.a. |
| Part d | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for appropriately transferring personnel. The customer control implementation statement should address the notification of customer-defined personnel/roles within the specified time period following personnel/transfer reassignment. |

### PS-6 Access Agreements (H)

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 and any time there is a change to the user's level of access].

| PS-6 | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter PS-6(b): <FedRAMP Assignment: at least annually> | |
| Parameter PS-6(c)(2): <FedRAMP Assignment: at least annually and any time there is a change to the user's level of access> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| PS-6 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for developing and documenting access agreements for customer-deployed resources. The customer control implementation statement should address the contents of these agreements. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for reviewing and updating access agreements. The customer control implementation statement should address the frequency with which access agreements are reviewed and updated. |
| Part c | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for ensuring that individuals requiring access to customer-deployed resources review and sign access agreements. The customer control implementation statement should address the requirements to sign access agreements prior to being granted access, and re-sign when the agreements have been updated and/or at a customer-defined frequency. |

### PS-7 Third-Party Personnel Security (H)

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: terminations: immediately; transfers: within twenty-four (24) hours]; and
5. Monitors provider compliance.

| PS-7 | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter PS-7(d)-1: *<Customer-defined personnel or roles>* | |
| Parameter PS-7(d)-2: *<*FedRAMP Assignment: terminations: immediately; transfers: within twenty-four (24) hours> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| PS-7 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for third-party personnel security. The customer control implementation statement should address the establishment of personnel security requirements for third-party providers (e.g., security roles and responsibilities). |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for third-party personnel security. The customer control implementation statement should address the requirement that third-part providers comply with customer-defined personnel security policies and procedures. |
| Part c | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for third-party personnel security. The customer control implementation statement should address the documentation of personnel security requirements defined in PS-07.a. |
| Part d | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for third-party personnel security. The customer control implementation statement should address the requirement that third-part providers notify customer-defined personnel/roles of any transfers/terminations of third-party personnel who possess customer credentials and/or badges within a customer-defined period of time. |
| Part e | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for third-party personnel security. The customer control implementation statement should address the monitoring of third-party provider compliance. |

### PS-8 Personnel Sanctions (H)

The organization:

1. Employs a formal sanctions process for personnel failing to comply with established information security policies and procedures; and
2. Notifies [FedRAMP Assignment: at a minimum, the ISSO and/or similar role within the organization] 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: *<Customer-defined>* | |
| Parameter PS-8(b)-1: <FedRAMP Assignment: at a minimum, the ISSO and/or similar role within the organization> | |
| Parameter PS-8(b)-2: *<Customer-defined time period>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| PS-8 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for establishing a sanctions process for customer employees failing to comply with information security policies and procedures. The customer control implementation statement should address the sanctions imposed for non-compliance. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for providing notifications when a formal employee sanctions process is initiated. The customer control implementation statement should address the customer-defined personnel/roles to be notified, the time period within which notification must occur, the identification of the sanctioned individual, and the reason for the sanction. |

## Risk Assessment (RA)

### RA-1 Risk Assessment Policy and Procedures (H)

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 annually]; and
   2. Risk assessment procedures [FedRAMP Assignment: at least annually or whenever a significant change occurs].

| RA-1 | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter RA-1(a): *<Customer-defined personnel or roles>* | |
| Parameter RA-1(b)(1): *<FedRAMP Assignment: at least annually>* | |
| Parameter RA-1(b)(2): *<FedRAMP Assignment: at least annually or whenever a significant change occurs>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| RA-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for developing, documenting, reviewing, updating, and disseminating risk assessment policy and procedures for the customer-deployed system. The customer control implementation statement should address the content of the policy (which must include purpose, scope, roles, responsibilities, management commitment, coordination, and compliance), procedures (which must facilitate the implementation of the policies and associated controls), the frequency of review, and the role(s) responsible. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for developing, documenting, reviewing, updating, and disseminating risk assessment policy and procedures for the customer-deployed system. The customer control implementation statement should address the content of the policy (which must include purpose, scope, roles, responsibilities, management commitment, coordination, and compliance), procedures (which must facilitate the implementation of the policies and associated controls), the frequency of review, and the role(s) responsible. |

### 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-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| RA-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for categorizing customer-deployed resources and the information contained. The customer control implementation statement should address the applicable Federal Laws, Executive Orders, directives, policies, regulations, standards, and guidance. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for documenting the results of the security categorization defined in RA-02.a. The customer control implementation statement should address the inclusion of these documented results (including supporting rationale) in the security plan for customer-deployed resources. |
| Part c | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for ensuring the security categorization decision is reviewed and approved. The customer control implementation statement should address the authorizing official (AO) or designated representative responsible for the review and approval. |

### RA-3 Risk Assessment (H)

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

RA-3 Additional FedRAMP Requirements and Guidance:

Requirement: Include all Authoring Officials and FedRAMP ISSOs.

1. 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 | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter RA-3(b): *<*Selection: security plan; risk assessment report; FedRAMP Assignment: security assessment report> | |
| Parameter RA-3(c): *<*FedRAMP Assignment: in accordance with OMB A-130 requirements or when a significant change occurs> | |
| Parameter RA-3(d): *<Customer-defined personnel or roles. Requirement: Include all Authoring Officials and FedRAMP ISSOs>* | |
| Parameter RA-3(e): *<*FedRAMP Assignment: in accordance with OMB A-130 requirements or when a significant change occurs> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| RA-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for conducting a risk assessment. The customer control implementation statement should address the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of customer-deployed resources and the information processed, stored, or transmitted. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for conducting a risk assessment. The customer control implementation statement should address the documentation of risk assessment results in the security plan, risk assessment report, and/or other customer-defined document. |
| Part c | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for conducting a risk assessment. The customer control implementation statement should address the frequency with which risk assessment results are reviewed. |
| Part d | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for conducting a risk assessment. The customer control implementation statement should address the dissemination of risk assessment results to customer-defined personnel/roles. |
| Part e | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for conducting a risk assessment. The customer control implementation statement should address the requirement to update the risk assessment at the customer-defined frequency and when there are significant changes to customer-deployed resources (including the identification of new threats and vulnerabilities) or other conditions that may impact the security state of the system. |

### 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: *<Customer-defined>;* Microsoft Azure | |
| Parameter RA-5(a): *<*FedRAMP Assignment: monthly operating system/infrastructure; monthly web applications and databases. Requirement: *An accredited independent assessor scans operating systems/infrastructure, web applications, and databases once annually.>* | |
| Parameter RA-5(d): *<*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> | |
| Parameter RA-5(e): *<Customer-defined personnel or roles. Requirement: To include the Risk Executive; for JAB authorizations to include FedRAMP ISSOs>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| RA-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (PaaS)**  Microsoft Azure implements this control for the operating systems supporting the PaaS environment.  Microsoft Azure scans for vulnerabilities in the Microsoft Azure virtual environment monthly or when a new vulnerability potentially affecting Microsoft Azure is identified and reported. These scans are used to ensure compliance with baseline configuration templates, validate that relevant patches are installed and identify vulnerabilities.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (PaaS)**  The customer is responsible for performing periodic vulnerability scanning on applications and software built on PaaS resources. The customer also may be responsible for performing a subset of vulnerability scanning activities on some customer-deployed PaaS resources. For example, Microsoft performs vulnerability scanning on the underlying infrastructure that supports SQL Database; however, customers are responsible for performing vulnerability scanning on the configuration and/or schema of the customer SQL Database deployment. The customer control implementation statement should address the frequency with which vulnerability scans are performed and for which resources/applications.  **Customer Responsibility (IaaS)**  The customer is responsible for performing periodic vulnerability scanning on all customer-deployed resources, including applications built on those resources. The customer control implementation statement should address how vulnerability scanning is performed, the frequency with which scanning occurs, and for which resources/applications. |
| Part b | **Microsoft Azure (PaaS)**  Microsoft Azure implements this control for the operating systems supporting the PaaS environment.  All vulnerability scanning tools used in the Microsoft Azure environment report risk results using Common Vulnerabilities and Exposures (CVE) values. The use of the CVE standards ensures interoperability among the tools as related to:   * Enumerating platforms, software flaws, and improper configurations; * Formatting and making transparent, checklists and test procedures; and * Measuring vulnerability impact   Microsoft Azure utilizes Tenable Nessus with the applicable plugins to run authenticated vulnerability scans on a representative sample of each OS role type. Nessus plugins are updated prior to scanning any hosts.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for employing vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process. The customer control implementation statement should address the use of standards for: enumerating platforms, software flaws, and improper configurations; formatting checklists and test procedures; and measuring vulnerability impact. |
| Part c | **Microsoft Azure (PaaS)**  Microsoft Azure implements this control for the operating systems supporting the PaaS environment.  The reports generated from the vulnerability scanning as part of the security controls assessment are analyzed to determine if there were any vulnerabilities that have been not been remediated in production. The risk triage process performed by Microsoft Azure determines if vulnerabilities identified in the scans are applicable to the non-public, custom-built Microsoft Azure environment.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for analyzing scan reports and results from security control assessments. The customer control implementation statement should address the criteria used in performing the analysis. |
| Part d | **Microsoft Azure (PaaS)**  Microsoft Azure implements this control for the operating systems supporting the PaaS environment.  Microsoft Azure remediates legitimate vulnerabilities, in accordance with organizational assessments of risk, using the following schedule:  Remediation for High Risk vulnerabilities is implemented within 30 days of the vulnerability identified.  Remediation for Moderate Risk vulnerabilities is implemented within 90 days of vulnerability the vulnerability identified.  Remediation for Low Risk vulnerabilities is implemented according to business risk justifications.  Vulnerability scans are conducted at the frequency described in part a, and using the tools described in part b of this control. Each of the Microsoft Azure service teams is responsible for patching the servers within their operational inventory.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (PaaS)**  The customer is responsible for remediating vulnerabilities in customer-deployed resources (to include applications, databases, and software) in accordance with the customer risk assessment. The customer control implementation statement should address customer-defined response times for remediation.  **Customer Responsibility (IaaS)**  The customer is responsible for remediating vulnerabilities in customer-deployed resources (to include applications, operating systems, databases, and software) in accordance with the customer risk assessment. The customer control implementation statement should address customer-defined response times for remediation. |
| Part e | **Microsoft Azure (PaaS)**  Microsoft Azure implements this control for the operating systems supporting the PaaS environment.  Microsoft Azure shares information obtained from the vulnerability scanning process with designated personnel to help eliminate similar vulnerabilities in other information systems.  Microsoft Azure shares information obtained from the vulnerability scanning process with designated personnel to help eliminate similar vulnerabilities in other information systems.  Azure Security Service Engineering provides a reporting interface to allow authorized Azure 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, percentages, CVE IDs, breakdowns of vulnerable hosts, and remediation steps etc.).  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for sharing information obtained from the vulnerability scanning process and security control assessments to help eliminate similar vulnerabilities across customer-deployed resources. The customer control implementation statement should address the customer-defined personnel/roles with which this information will be shared. |

#### 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-5 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>;* Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| RA-5 (1) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (PaaS)**  Microsoft Azure implements this control for the operating systems supporting the PaaS environment.  The vulnerability scanning tools used within the Microsoft Azure environment (for OS scans, Nessus) are updated before each scan of the environment is conducted. The tools release new vulnerability definitions as needed following the publication of Common Vulnerability and Exposures (CVE) information. The update is completed by the engineering conducting the scans prior to initiation of the scan.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for employing the capability to update vulnerability scanning tools. The customer control implementation statement should address the capability of the customer's vulnerability scanning tools to readily update the vulnerabilities to be scanned. |

#### 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-5 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>;* Microsoft Azure | |
| Parameter RA-5(2): *<FedRAMP Assignment: 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| RA-5 (2) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (PaaS)**  Microsoft Azure implements this control for the operating systems supporting the PaaS environment.  The vulnerability scanning tools used within the Microsoft Azure environment (for OS scans, Nessus) are updated before each scan of the environment is conducted. The tools release new vulnerability definitions as needed following the publication of Common Vulnerability and Exposures (CVE) information. The update is completed by the engineering conducting the scans prior to initiation of the scan.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for updating the list of vulnerabilities scanned. The customer control implementation statement should address the requirement that scanned vulnerabilities are updated prior to a new scan, when new vulnerabilities are identified and reported, and/or at the customer-defined frequency. |

#### 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-5 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>;* Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| RA-5 (3) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (PaaS)**  Microsoft Azure implements this control for the operating systems supporting the PaaS environment.  All vulnerability scanning tools used to support Microsoft Azure (for OS scans, Nessus) use Common Vulnerability and Exposures (CVE) information to develop their scanning engines. As a result, each of these tools ensures a breadth and depth of coverage, as recognized by the information security community.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for employing vulnerability scanning procedures that identify the breadth and depth of coverage. The customer control implementation statement should address the procedures used to identify the customer-deployed resources scanned and vulnerabilities checked. |

#### RA-5 (4) Control Enhancement (H)

The organization determines what information about the information system is discoverable by adversaries and subsequently takes [FedRAMP Assignment: notify appropriate service provider personnel and follow procedures for organization and service provider-defined corrective actions].

| RA-5 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter RA-5 (4): <FedRAMP Assignment: notify appropriate service provider personnel and follow procedures for organization and service provider-defined corrective actions> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| RA-5 (4) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for taking action in response to discoverable information. The customer control implementation statement should address the identification of customer information that is discoverable by adversaries and the customer-defined corrective actions taken subsequently. |

#### 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-5 (5) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>;* Microsoft Azure | |
| Parameter RA-5(5)-1: <FedRAMP Assignment: operating systems, databases, web applications> | |
| Parameter RA-5(5)-2: <FedRAMP Assignment: all scans> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| RA-5 (5) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (PaaS)**  Microsoft Azure implements this control for the operating systems supporting the PaaS environment.  All vulnerability scans conducted on the Microsoft Azure environment are ‘authenticated scans’ which use privileged accounts for authentication. The engineer conducting the scans is responsible for ensuring that the scan executed using a privileged account to ensure thorough scanning.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for implementing privileged access for vulnerability scanning. The customer control implementation statement should address the identified customer-deployed resources requiring privileged access to execute customer-defined vulnerability scanning activities. |

#### 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-5 (6) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>;* Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| RA-5 (6) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (PaaS)**  Microsoft Azure implements this control for the operating systems supporting the PaaS environment.  For all asset types, Microsoft Azure performs vulnerability scans as described in RA-5. Scan results for OS scans are compared over time to determine trends in vulnerability scan results, such as number of new vulnerabilities each month or total number of open vulnerabilities.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for employing automated mechanisms for vulnerability trend analysis. The customer control implementation statement should address the mechanisms used to compare the results of vulnerability scans over time to determine vulnerability trends in customer-deployed resources. |

#### 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-5 (8) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>;* Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| RA-5 (8) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (PaaS)**  Microsoft Azure implements this control for the operating systems supporting the PaaS environment.  Microsoft Azure Security’s PAVC team is responsible for reviewing newly-identified high findings and determining if they could have possibly been exploited.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for reviewing historic audit logs. The customer control implementation statement should address the use of these logs to determine if a vulnerability identified within customer-deployed resources has been previously exploited. |

#### RA-5 (10) Control Enhancement (H)

The organization correlates the output from vulnerability scanning tools to determine the presence of multi-vulnerability/multi-hop attack vectors.

RA-5 (10) Additional FedRAMP Requirements and Guidance:

Guidance: If multiple tools are not used, this control is not applicable.

| RA-5 (10) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| RA-5 (10) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for correlating vulnerability scanning information. The customer control implementation statement should address the vulnerability scanning data correlated to determine the presence of multi-vulnerability/multi-hop attack vectors. |

## System and Services Acquisition (SA)

### SA-1 System and Services Acquisition Policy and Procedures (H)

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 annually]; and
   2. System and services acquisition procedures [FedRAMP Assignment: at least annually or whenever a significant change occurs].

| SA-1 | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter SA-1(a): *<FedRAMP Assignment: organization-defined personnel or roles>* | |
| Parameter SA-1(b)(1): *<FedRAMP Assignment: at least annually>* | |
| Parameter SA-1(b)(2): *<FedRAMP Assignment: at least annually or whatever a significant change occurs>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| SA-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for developing, documenting, reviewing, updating, and disseminating system and services acquisition policy and procedures for customer-deployed resources. The customer control implementation statement should address the content of the policy (which must include purpose, scope, roles, responsibilities, management commitment, coordination, and compliance), procedures (which must facilitate the implementation of the policies and associated controls), the frequency of review, and the role(s) responsible. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for developing, documenting, reviewing, updating, and disseminating system and services acquisition policy and procedures for customer-deployed resources. The customer control implementation statement should address the content of the policy (which must include purpose, scope, roles, responsibilities, management commitment, coordination, and compliance), procedures (which must facilitate the implementation of the policies and associated controls), the frequency of review, and the role(s) responsible. |

### 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: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SA-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for allocating resources for information security. The customer control implementation statement should address the security requirements for customer-deployed resources in mission/business process planning. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for allocating resources for information security. The customer control implementation statement should address the documentation and allocation of resources required to protect customer-deployed resources as part of capital planning and investment control. |
| Part c | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for allocating resources for information security. The customer control implementation statement should address the inclusion of a discrete line item for information security in programming and budgeting documentation. |

### 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: *<Customer-defined>,* Microsoft Azure | |
| Parameter SA-3(a): *<FedRAMP Assignment: organization-defined system development life cycle>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SA-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  Microsoft implements life cycle support for Microsoft Azure through its SDL process that is followed for all engineering and development projects. 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 during the SDL.  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.  For more details on the SDL process, please refer to http://www.microsoft.com/security/sdl/.  **Customer Responsibility (PaaS)**  The customer is responsible for managing customer-deployed resources (to include applications, databases, and software) using a system development life cycle (SDLC). The customer control implementation statement should address how the customer-defined SDLC process incorporates information security considerations.  **Customer Responsibility (IaaS)**  The customer is responsible for managing customer-deployed resources (to include applications, operating systems, databases, and software) using a system development life cycle (SDLC). The customer control implementation statement should address how the customer-defined SDLC process incorporates information security considerations. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure follows the SDL process, which includes defining security roles and responsibilities throughout the SDL process.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for managing customer-deployed resources using a system development life cycle (SDLC). The customer control implementation statement should address the definition and documentation of information security roles and responsibilities throughout the SDLC. |
| Part c | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure follows the SDL process, which includes identifying individuals with security roles and responsibilities throughout the SDL process.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for managing customer-deployed resources using a system development life cycle (SDLC). The customer control implementation statement should address the identification of individuals having information security roles and responsibilities defined in SA-03.b. |
| Part d | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for managing customer-deployed resources using a system development life cycle (SDLC). The customer control implementation statement should address the integration of the customer's information security risk management process into SDLC activities. |

### 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-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SA-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for implementing an acquisition process for customer-deployed resources (to include applications, operating systems, databases, and software) in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and any customer-defined mission/business needs. The customer control implementation statement should address the inclusion of security-related functional, strength, assurance, and documentation requirements in the acquisition contract. The acquisition contract should also address the requirements for protecting security-related documentation, a description of the customer's development and operating environments, and the acceptance criteria for the contract. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for implementing an acquisition process for customer-deployed resources (to include applications, operating systems, databases, and software) in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and any customer-defined mission/business needs. The customer control implementation statement should address the inclusion of security-related functional, strength, assurance, and documentation requirements in the acquisition contract. The acquisition contract should also address the requirements for protecting security-related documentation, a description of the customer's development and operating environments, and the acceptance criteria for the contract. |
| Part c | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for implementing an acquisition process for customer-deployed resources (to include applications, operating systems, databases, and software) in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and any customer-defined mission/business needs. The customer control implementation statement should address the inclusion of security-related functional, strength, assurance, and documentation requirements in the acquisition contract. The acquisition contract should also address the requirements for protecting security-related documentation, a description of the customer's development and operating environments, and the acceptance criteria for the contract. |
| Part d | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for implementing an acquisition process for customer-deployed resources (to include applications, operating systems, databases, and software) in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and any customer-defined mission/business needs. The customer control implementation statement should address the inclusion of security-related functional, strength, assurance, and documentation requirements in the acquisition contract. The acquisition contract should also address the requirements for protecting security-related documentation, a description of the customer's development and operating environments, and the acceptance criteria for the contract. |
| Part e | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for implementing an acquisition process for customer-deployed resources (to include applications, operating systems, databases, and software) in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and any customer-defined mission/business needs. The customer control implementation statement should address the inclusion of security-related functional, strength, assurance, and documentation requirements in the acquisition contract. The acquisition contract should also address the requirements for protecting security-related documentation, a description of the customer's development and operating environments, and the acceptance criteria for the contract. |
| Part f | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for implementing an acquisition process for customer-deployed resources (to include applications, operating systems, databases, and software) in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and any customer-defined mission/business needs. The customer control implementation statement should address the inclusion of security-related functional, strength, assurance, and documentation requirements in the acquisition contract. The acquisition contract should also address the requirements for protecting security-related documentation, a description of the customer's development and operating environments, and the acceptance criteria for the contract. |
| Part g | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for implementing an acquisition process for customer-deployed resources (to include applications, operating systems, databases, and software) in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and any customer-defined mission/business needs. The customer control implementation statement should address the inclusion of security-related functional, strength, assurance, and documentation requirements in the acquisition contract. The acquisition contract should also address the requirements for protecting security-related documentation, a description of the customer's development and operating environments, and the acceptance criteria for the contract. |

#### 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-4 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>,* Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SA-4 (1) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure implements this control for all underlying infrastructure supporting the Microsoft Azure service. A full description of Microsoft’s implementation can be found in the SSP.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for obtaining a description of the security controls to be employed from the developer of the corresponding customer-deployed resource(s). The customer control implementation statement should address the functional properties of the security controls referenced above. Note: Microsoft Azure hosts the customer-deployed system. The customer can find a description of the security controls employed by Azure in the Microsoft Azure section above. |

#### SA-4 (2) Control Enhancement (H)

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): at a minimum to include security-relevant external system interfaces; high-level design; low-level design; source code or network and data flow diagram; [organization-defined design/implementation information]]at [Assignment: organization-defined level of detail].

| SA-4 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>,* Microsoft Azure | |
| Parameter SA-4-1: *<FedRAMP Selection (one or more): at a minimum to include security-relevant external system interfaces; high-level design; low-level design; source code or network and data flow diagram>* | |
| Parameter SA-4-2: *<FedRAMP Assignment: organization-defined design/implementation information>* | |
| Parameter SA-4-3: *<FedRAMP Assignment: organization-defined level of detail>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SA-4 (2) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure implements this control for all underlying infrastructure supporting the Microsoft Azure service. A full description of Microsoft’s implementation can be found in the SSP.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for obtaining design and implementation information for the security controls to be employed from the developer of the corresponding customer-deployed resource(s). The customer control implementation statement should address the inclusion of security-relevant external system interfaces; high-level design; low-level design; source code schematics; and any customer-defined design/implementation information at an organization-defined level of detail in the design and implementation information. Note: Microsoft Azure hosts the customer-deployed system. The customer can find a description of the security controls employed by Azure in the Microsoft Azure section above. |

#### 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-4 (8) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>,* Microsoft Azure | |
| Parameter SA-4(8): *<FedRAMP Assignment: at least the minimum requirement as defined in control CA-7>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SA-4 (8) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (PaaS)**  Microsoft Azure implements this control for the operating systems supporting the PaaS environment.  Microsoft Azure continuously monitors control effectiveness of organizations from which Microsoft Azure inherits security controls. See CA-7 for additional information.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for obtaining a plan for continuously monitoring security control effectiveness from the developer of the corresponding customer-deployed resource(s). The customer control implementation statement should address the customer-defined level of detail required in the plan. Note: Microsoft Azure hosts the customer-deployed system. The customer can find a description of the security controls employed by Azure in the Microsoft Azure section above. |

#### 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-4 (9) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>,* Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SA-4 (9) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (PaaS)**  Microsoft Azure implements this control for the operating systems supporting the PaaS environment.  Microsoft Azure follows the SDL process, which includes as part of the design phase the identification of the functions, ports, protocols, and services intended for organizational use.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for obtaining a description of the identified ports, protocols, and services intended for use from the developer of the corresponding customer-deployed resource(s). The customer control implementation statement should address the fact that the developer must identify such ports, protocols, and services early in the SDLC. Note: Microsoft Azure hosts the customer-deployed system. The customer can find a description of the security controls employed by Azure in the Microsoft Azure section above. |

#### 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-4 (10) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>,* Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SA-4 (10) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for employing FIPS 201-approved technology products, in order to support Personal Identity Verification (PIV) capability. The customer control implementation statement should address the technology employed in the customer-deployed system ensuring that it appears on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability. Note: if the customer does not deploy PIV credentials this control is not applicable. |

### SA-5 Information System Documentation (H)

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 [FedRAMP Assignment: at a minimum, the ISSO (or similar role within the organization)].

| SA-5 | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>,* Microsoft Azure | |
| Parameter SA-5(c): *<FedRAMP Assignment: organization-defined actions>* | |
| Parameter SA-5(e): *<FedRAMP Assignment: at a minimum, the ISSO (or similar role within the organization)>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SA-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (PaaS)**  Microsoft Azure implements this control for the operating systems supporting the PaaS environment.  Microsoft Azure service teams maintain, secure, manage, and store information system documentation, including documentation regarding:   * Secure configuration, installation, and operation of the information system; * Effective use and maintenance of security features/functions; and * Known vulnerabilities regarding configuration and use of administrative (i.e. privileged) functions   This documentation is stored in each service team’s SharePoint site and made available to service team administrators. Documentation for externally-provided software (scanning tools) is available online at vendor websites.  Acquisition of hardware and associated documentation is inherited from Microsoft Azure.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (PaaS)**  The customer is responsible for obtaining administrator documentation for customer-deployed resources (to include applications, databases, and software). The customer control implementation statement should address the requirement that the documentation describes: secure configuration, installation, and operation of the customer-deployed resources; effective use and maintenance of security functions/mechanisms; known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions.  **Customer Responsibility (IaaS)**  The customer is responsible for obtaining administrator documentation for customer-deployed resources (to include applications, operating systems databases, and software). The customer control implementation statement should address the requirement that the documentation describes: secure configuration, installation, and operation of the customer-deployed resources; effective use and maintenance of security functions/mechanisms; known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions. |
| Part b | **Microsoft Azure (PaaS)**  Microsoft Azure implements this control for the operating systems supporting the PaaS environment.  Microsoft Azure has extensive user-facing documentation on all aspects of the system, including security functions. This documentation is available online at the following address: <https://msdn.microsoft.com/library/azure/>  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for obtaining user documentation for customer-deployed resources. The customer control implementation statement should address the requirement that the documentation describes: user-accessible security functions/mechanisms and how to effectively use them; methods for user interaction, which enables individuals to use the customer-deployed resources in a more secure manner; user responsibilities in maintaining the security of the customer-deployed resources. |
| Part c | **Microsoft Azure (PaaS)**  Microsoft Azure implements this control for the operating systems supporting the PaaS environment.  Per acquisition policy, attempts are made to obtain documentation if it is not initially provided. Documentation for externally-provided software (scanning tools) is available online at vendor websites.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for documenting attempts to obtain administrator and/or user documentation for customer-deployed resources when such documentation is not available/nonexistent. The customer control implementation statement should address the customer-defined actions taken in response to these attempts. |
| Part d | **Microsoft Azure (PaaS)**  Microsoft Azure implements this control for the operating systems supporting the PaaS environment.  Microsoft Azure service teams maintain, secure, manage, and store information system documentation, including documentation regarding:   * Secure configuration, installation, and operation of the information system; * Effective use and maintenance of security features/functions; and * Known vulnerabilities regarding configuration and use of administrative (i.e. privileged) functions   This documentation is stored in each service team’s SharePoint site and made available to service team administrators. The documentation is secured via SharePoint's internal security mechanisms.  Acquisition of hardware and associated documentation is inherited from Microsoft Azure. Documentation for externally-provided software (scanning tools) is available online at vendor websites.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for protecting administrator and user documentation for customer-deployed resources. The customer control implementation statement should address the protection mechanisms used in accordance in with the organization’s risk management strategy. |
| Part e | **Microsoft Azure (PaaS)**  Microsoft Azure implements this control for the operating systems supporting the PaaS environment.  Microsoft Azure service teams maintain, secure, manage, and store information system documentation, including documentation regarding:   * Secure configuration, installation, and operation of the information system; * Effective use and maintenance of security features/functions; and * Known vulnerabilities regarding configuration and use of administrative (i.e. privileged) functions   This documentation is stored in each service team’s SharePoint site and made available to service team administrators. The documentation is secured via SharePoint's internal security mechanisms.  Acquisition of hardware and associated documentation is inherited from Microsoft Azure. Documentation for externally-provided software (scanning tools) is available online at vendor websites.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for distributing documentation for customer-deployed resources. The customer control implementation statement should address the means by which the documents identified in SA-05.a, SA-05.b and SA-05.c are distributed to customer-defined personnel/roles. |

### 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-8 | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>,* Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SA-8 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure has a mature SDL process that is followed for all engineering and development projects. The Microsoft SDL process implements standard security engineering principles across all of Microsoft’s online services’ systems. The System Owner is responsible for ensuring that the SDL process is followed for all engineering initiatives associated with Microsoft Azure.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for applying security engineering principles to customer-deployed resources. The customer control implementation statement should address how these principles are applied in the specification, design, development, implementation, and modification of customer-deployed resources. |

### 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](https://www.fedramp.gov/resources/documents)

| SA-9 | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>,* Microsoft Azure | |
| Parameter SA-9(a): *<FedRAMP Assignment:* FedRAMP Security Controls Baseline(s) if Federal information is processed or stored within the external system> | |
| Parameter SA-9(c): *<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*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SA-9 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  Microsoft requires all third parties (external information system services) who are engaged with Azure to sign a Microsoft Master Vendor Agreement (MMVA). The MMVA 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 MMVA 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, Microsoft Azure signs ISAs with external information systems as required by CA-3; ISAs define Microsoft Azure oversight and roles/responsibilities. (At this time, Microsoft Azure does not have any dependencies on information systems external to Microsoft that require ISAs.)  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for requiring that external service providers comply with the customer's information security requirements and employ customer-defined security controls. The customer control implementation statement should address how the security controls are used in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure signs ISAs with external information systems as required by CA-3; ISAs define Microsoft Azure 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 Microsoft Azure ISAs and continuous monitoring, which includes reports on ISA oversight.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for defining and documenting government oversight and user responsibilities and roles with regard to external system services. The customer control implementation statement should address all parties involved in assuring the external service provider is compliant and document their roles and responsibilities. |
| Part c | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure compliance monitoring processes, methods and techniques are applied to customer data and access control data and are documented in ISAs and executed by Microsoft Azure Security.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for continuously monitoring external service providers. The customer control implementation statement should address the customer-defined process, methods, and techniques used to monitor security control compliance by external service providers on an ongoing basis. |

#### 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: *<Customer-defined>,* Microsoft Azure | |
| Parameter SA-9(1)(b): *<FedRAMP Assignment: organization-defined personnel or roles>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SA-9 (1) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure does not consider any information security services to be outsourced as they are defined in the supplemental guidance for the requirement. If any services were to be outsourced after receiving a FedRAMP P-ATO, Microsoft Azure Security would complete an assessment of risk and follow FedRAMP change management processes.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for conducting a risk assessment prior to acquiring or outsourcing dedicated information security services. The customer control implementation statement should address the risk assessment process used. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure's engaging team(s) will ensure the acquisition or outsourcing of dedicated information security services is approved by the JAB or DoD component.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for obtaining approval of acquisitions or outsourcing of dedicated information security services. The customer control implementation statement should address the customer-defined personnel/roles responsible for approval. |

#### 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-9 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>,* Microsoft Azure | |
| Parameter SA-9(2): *<FedRAMP Assignment: All external systems where Federal information is processed or stored>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SA-9 (2) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure requires the system to provide information about the functions, ports, protocols and other services required for the use of such services as part of the process of establishing a connection to an external system.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for requiring external service providers to identify the functions, ports, protocols and other services required for the use of that service. The customer control implementation statement should address external providers of system services and the functions, ports, protocols and services leveraged in order to utilize those external 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-9 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>,* Microsoft Azure | |
| Parameter SA-9(4)-1: *<FedRAMP Assignment: organization-defined security safeguards>* | |
| Parameter SA-9(4)-2: *<FedRAMP Assignment: all external systems where Federal information is processed or stored>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SA-9 (4) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure does not have any dependencies on information systems external to Microsoft at this time. If Federal customers move data between Microsoft Azure and external systems, those customers are responsible for ensuring that the external systems have security safeguards that are consistent with and reflect customer interests.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for employing safeguards to ensure the interests of external service providers are consistent with and reflect those of the customer. The customer control implementation statement should address the external service providers selected and the customer-defined security safeguards employed. |

#### 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-9 (5) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>,* Microsoft Azure | |
| Parameter SA-9(5)-1: *<FedRAMP Assignment: information processing, information data, AND information services>* | |
| Parameter SA-9(5)-2: *<FedRAMP Assignment: organization-defined locations>* | |
| Parameter SA-9(5)-3: *<FedRAMP Assignment: organization-defined requirements or conditions>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SA-9 (5) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure restricts the location of all services and data within the accreditation boundary to Microsoft Azure Continental United States datacenters. When a government customer offering is purchased, the customer is provisioned into continental United States datacenters.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for restricting the location of information processing, storage, and service. The customer control implementation statement should address how the customer restricts information process, information/data, and information system services to customer-defined locations based on customer-defined requirements/conditions. |

### 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: *<Customer defined>,* Microsoft Azure | |
| Parameter SA-10(a): *<FedRAMP Assignment: development, implementation, AND operation>* | |
| Parameter SA-10(b): *<FedRAMP Assignment: organization-defined configuration items under configuration management>* | |
| Parameter SA-10(e): *<FedRAMP Assignment: organization-defined 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SA-10 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (PaaS)**  Microsoft Azure implements this control for the operating systems supporting the PaaS environment.  All Microsoft Azure software developers are required to follow the Microsoft Azure Configuration Management Plan and Microsoft’s corporate Security Development Lifecycle (SDL) during information system design, development, implementation, and operation.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (PaaS)**  The customer is responsible for requiring the developer of customer-deployed resources (to include applications, databases, and software) to utilize configuration management. The customer control implementation statement should address the requirement that the developer perform configuration management during the design, development, implementation, and operation of the resources provided.  **Customer Responsibility (IaaS)**  The customer is responsible for requiring the developer of customer-deployed resources (to include applications, operating systems, databases, and software) to utilize configuration management. The customer control implementation statement should address the requirement that the developer perform configuration management during the design, development, implementation, and operation of the resources provided. |
| Part b | **Microsoft Azure (PaaS)**  Microsoft Azure implements this control for the operating systems supporting the PaaS environment.  Microsoft Azure developers leverage Source Depot and Git to document, manage and control the integrity of changes in the development environment. These tools provide technical enforcement of documented change management processes and the SDL. Among other features, they prevent changes to configuration items that are not tied to an approved change request.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for requiring the developer of customer-deployed resources to utilize configuration management. The customer control implementation statement should address the requirement that the developer document, manage, and control the integrity of changes to customer-defined configuration items. |
| Part c | **Microsoft Azure (PaaS)**  Microsoft Azure implements this control for the operating systems supporting the PaaS environment.  Developers of Microsoft Azure implement only approved changes to the system. The service teams follow the configuration management processes when implementing changes. Changes are approved through Source Depot, Git, or TFS.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for requiring the developer of customer-deployed resources to utilize configuration management. The customer control implementation statement should address the requirement that the developer implements only organization-approved changes to the resources provided. |
| Part d | **Microsoft Azure (PaaS)**  Microsoft Azure implements this control for the operating systems supporting the PaaS environment.  The service team tracks all approved changes in Source Depot, Git, or TFS. As part of change management processes, other documentation such as the SSP or user and administrative documentation is updated if applicable.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for requiring the developer of customer-deployed resources to utilize configuration management. The customer control implementation statement should address the requirement that the developer to document approved changes to the resources provided and the potential security impacts of such changes. |
| Part e | **Microsoft Azure (PaaS)**  Microsoft Azure implements this control for the operating systems supporting the PaaS environment.  Microsoft Azure service team developers track security flaws and flaw resolution during the development process using TFS. Any identified flaws, whether discovered by a human or by the automated tools described in SA-3 part a, have a corresponding bug opened in TFS. 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, Microsoft Azure Security, and FedRAMP.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for requiring the developer of customer-deployed resources to utilize configuration management. The customer control implementation statement should address the requirement that the developer track security flaws and flaw resolution within the resources provided and report findings to customer-defined personnel. |

#### 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: *<Customer-defined>,* Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SA-10 (1) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (PaaS)**  Microsoft Azure implements this control for the operating systems supporting the PaaS environment.  As part of the development process, builds are approved through QE and TFS, then signed. Only signed builds are allowed to be deployed within the environment.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (PaaS)**  The customer is responsible for requiring the developer of customer-deployed resources (to include applications, databases, and software) to utilize configuration management. The customer control implementation statement should address the requirement that the developer enables integrity verification of resources provided.  **Customer Responsibility (IaaS)**  The customer is responsible for requiring the developer of customer-deployed resources (to include applications, operating systems, databases, and software) to utilize configuration management. The customer control implementation statement should address the requirement that the developer enables integrity verification of resources provided. |

### 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: *<Customer-defined>,* Microsoft Azure | |
| Parameter SA-11(b)-1: *<FedRAMP Selection (one or more): unit; integration; system; regression testing/evaluation>* | |
| Parameter SA-11(b)-2: *<FedRAMP Assignment: organization-defined depth and coverage>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SA-11 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (PaaS)**  Microsoft Azure implements this control for the operating systems supporting the PaaS environment.  In accordance with Microsoft’s corporate Security Development Lifecycle (SDL), security testing occurs in several phases throughout the SDL process. Specifically, security testing occurs during the following phases:   * Phase 3 – Implementation * Phase 4 – Verification * Phase 5 – Release   **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (PaaS)**  The customer is responsible for requiring the developer of customer-deployed resources (to include applications, databases, and software) to perform testing and evaluation. The customer control implementation statement should address the requirement that the developer create and implement a security assessment plan.  **Customer Responsibility (IaaS)**  The customer is responsible for requiring the developer of customer-deployed resources (to include applications, operating systems, databases, and software) to perform testing and evaluation. The customer control implementation statement should address the requirement that the developer create and implement a security assessment plan. |
| Part b | **Microsoft Azure (PaaS)**  Microsoft Azure implements this control for the operating systems supporting the PaaS environment.  The results of the security tests are documented in tickets opened in TFS. Remediation work and successful retesting is documented in the same ticket.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for requiring the developer of customer-deployed resources to perform testing and evaluation. The customer control implementation statement should address the requirement that the developer perform unit, integration, system, and/or regression testing/evaluation at the customer-defined depth and coverage. |
| Part c | **Microsoft Azure (PaaS)**  Microsoft Azure implements this control for the operating systems supporting the PaaS environment.  The results of the security tests are documented in tickets opened in TFS. Remediation work and successful retesting is documented in the same ticket.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for requiring the developer of customer-deployed resources to perform testing and evaluation. The customer control implementation statement should address the requirement that the developer produce evidence of the execution of the security assessment plan and the results of testing/evaluation. |
| Part d | **Microsoft Azure (PaaS)**  Microsoft Azure implements this control for the operating systems supporting the PaaS environment.  The Microsoft Azure system owner is responsible for ensuring that all system development and maintenance activities are performed in accordance with the Microsoft SDL process.  A formal review process is implemented to ensure that new or modified source code authored by Microsoft’s online services staff is developed in a secure fashion, no malicious code has been introduced into the system, and that proper coding practices are followed. The reviewers’ names, review dates, and review results are documented in TFS, 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 described in SA-3 part a and requires that all high vulnerabilities get remediated before the system will be released to production. A ticket for each vulnerability is opened in TFS and tracked to resolution.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for requiring the developer of customer-deployed resources to perform testing and evaluation. The customer control implementation statement should address the requirement that the developer implement a verifiable flaw remediation process. |
| Part e | **Microsoft Azure (PaaS)**  Microsoft Azure implements this control for the operating systems supporting the PaaS environment.  As part of the SDL process, flaws identified during testing are remediated prior to release. The results of the security tests are documented in tickets opened in TFS. Remediation work and successful retesting is documented in the same ticket.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for requiring the developer of customer-deployed resources to perform testing and evaluation. The customer control implementation statement should address the requirement that the developer correct flaws identified during security testing/evaluation. |

#### 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: *<Customer-defined>,* Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SA-11 (1) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (PaaS)**  Microsoft Azure implements this control for the operating systems supporting the PaaS environment.  Code reviews are performed as part of the Microsoft SDL, including automated tools such as FxCop and StyleCop.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (PaaS)**  The customer is responsible for requiring the developer of customer-deployed resources (to include applications, databases, and software) to perform testing and evaluation. The customer control implementation statement should address the requirement that the developer employ static code analysis tools to identify common flaws and document the results of the analysis.  **Customer Responsibility (IaaS)**  The customer is responsible for requiring the developer of customer-deployed resources (to include applications, operating systems, databases, and software) to perform testing and evaluation. The customer control implementation statement should address the requirement that the developer employ static code analysis tools to identify common flaws and document the results of the analysis. |

#### 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: *<Customer-defined>,* Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SA-11 (2) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (PaaS)**  Microsoft Azure implements this control for the operating systems supporting the PaaS environment.  In accordance with Microsoft’s corporate Security Development Lifecycle (SDL), security testing occurs in several phases throughout the SDL process. Specifically, security testing occurs during the following phases:   * Phase 3 – Implementation * Phase 4 – Verification * Phase 5 – Release   Testing at the release phase is performed on the as-built system. Vulnerabilities found at the release testing phase are tracked and remediated as discussed in SA-11.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (PaaS)**  The customer is responsible for requiring the developer of customer-deployed resources (to include applications, databases, and software) to perform testing and evaluation. The customer control implementation statement should address the requirement that the developer perform threat and vulnerability analyses and subsequent testing/evaluation of the as-built resources provided.  **Customer Responsibility (IaaS)**  The customer is responsible for requiring the developer of customer-deployed resources (to include applications, operating systems, databases, and software) to perform testing and evaluation. The customer control implementation statement should address the requirement that the developer perform threat and vulnerability analyses and subsequent testing/evaluation of the as-built resources provided. |

#### 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: *<Customer-defined>,* Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SA-11 (8) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (PaaS)**  Microsoft Azure implements this control for the operating systems supporting the PaaS environment.  Code reviews are performed as part of the Microsoft SDL, including use of the automated dynamic code analysis tools described in SA-3 part a.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (PaaS)**  The customer is responsible for requiring the developer of customer-deployed resources (to include applications, databases, and software) to perform testing and evaluation. The customer control implementation statement should address the requirement that the developer employ dynamic code analysis tools to identify common flaws and document the results of the analysis.  **Customer Responsibility (IaaS)**  The customer is responsible for requiring the developer of customer-deployed resources (to include applications, operating systems, databases, and software) to perform testing and evaluation. The customer control implementation statement should address the requirement that the developer employ dynamic code analysis tools to identify common flaws and document the results of the analysis. |

### SA-12 Supply Chain Protection (H)

The organization protects against supply chain threats to the information system, system component, or information system service by employing [FedRAMP Assignment: organization and service provider-defined personnel security requirements, approved HW/SW vendor list/process, and secure SDLC procedures] as part of a comprehensive, defense-in-breadth information security strategy.

| SA-12 | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>,* Microsoft Azure | |
| Parameter SA-12: *<FedRAMP Assignment: organization and service* provider-defined personnel security requirements, approved HW/SW vendor list/process, and secure SDLC 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SA-12 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure’s Hardware Supply Management (HSM) group consists of four unique teams; Release Management, Procurement and Spares, Planning, and Quality, each contributing to protect Azure from threats to the Supply Chain. During the initial supply chain phase of the system development life cycle, the Procurement team protects against supply chain threats by facilitating the creation of the purchase order to our suppliers ensuring consistency in approach, component forecasting and positioning, manufacturing, and packaging to delivery. This team along with our Release Management team liaisons define specifications and the delivery mechanism of those specifications to the suppliers. Routine business reviews are conducted with our suppliers representing the needs and concerns of all Azure business groups. The Planning team works to preposition inventory to allow for rapid delivery on approved spend, thereby reducing the required forecasting time for the Azure business groups. This team works to support Azure business groups on standards definition and service capability. A key function of this team is to protect against any threats posed by suppliers during manufacturing by ensuring adherence to standard supply chain methodologies and process adherence.  System integration or upon delivery of systems to our data centers for deployment; the Deployment Quality team works to ensure final delivery of the system to the Azure business group is done on-time and free of defects. Working in conjunction with the Supply Chain Automation team, these teams monitor performance metrics, capture business group feedback, and lead cross-functional Supply Chain projects for Azure. As systems move into the operations and maintenance phase of the life cycle, the Supplier Quality team protects Azure by managing and facilitating the supplier complaint process to drive root cause and corrective action within the suppliers’ supply chain. Supplier scorecards have been developed to allow Azure to compare and visibly monitor the performance of our supply base utilizing a balanced scorecard approach. This team also works directly with Azure business groups to ensure warranty entitlement and holds the supply base accountable for producing a quality product. The Spares Management team protects against supply chain threats by managing the determination and execution of obtaining spare components to support deployed devices within our data centers. The team works with our Release Management team who works directly with our suppliers to determine failure rates for components and acceptable field replacement parts. Parts are spared to significantly reduce downtime of production equipment during a trouble-shooting scenario, helping to ensure site up for our business.  In order to ensure security of the supply chain and protection against threats, below are some of the practices implemented by Azure:   * To the maximum extent possible, use well-established suppliers (e.g., MS, Juniper, Cisco, EMC, etc.) with a proven track record to secure supply chain management. * All hardware and software be ordered direct from the manufacturer or through manufacturer certified and approved distribution partners as directed by manufacturer. * Have established Service Level Agreements with critical providers to ensure that additional spare parts and maintenance activities are performed in a timely manner.   **Customer Responsibility (PaaS)**  The customer is responsible for protecting customer-deployed resources (to include applications, databases, and software) against supply chain threats. The customer control implementation statement should address the customer-defined security safeguards employed to protect against supply chain threats as part of a comprehensive, defense-in-breadth information security strategy.  **Customer Responsibility (IaaS)**  The customer is responsible for protecting customer-deployed resources (to include applications, operating systems, databases, and software) against supply chain threats. The customer control implementation statement should address the customer-defined security safeguards employed to protect against supply chain threats as part of a comprehensive, defense-in-breadth information security strategy. |

### SA-15 Development Process, Standards, and Tools (H)

The organization:

1. Requires the developer of the information system, system component, or information system service to follow a documented development process that:
   1. Explicitly addresses security requirements;
   2. Identifies the standards and tools used in the development process;
   3. Documents the specific tool options and tool configurations used in the development process; and
   4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and
2. Reviews the development process, standards, tools, and tool options/configurations [FedRAMP Assignment: as needed and as dictated by the current threat posture] to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy [FedRAMP Assignment: organization and service provider- defined security requirements].

| SA-15 | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>,* Microsoft Azure | |
| Parameter SA-15 (b)-1: *<FedRAMP Assignment: as needed and as dictated by the current threat posture>* | |
| Parameter SA-15 (b)-2: *<FedRAMP Assignment: organization and service provider-defined security 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SA-15 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (PaaS)**  The customer is responsible for requiring developers of customer-deployed resources (to include applications, databases, and software) to follow a documented development process. The customer control implementation statement should address how the development process: explicitly addresses security requirements; identifies standards and tools used; documents the specific tool options and configurations used; documents, manages, and ensures the integrity of changes to the process and/or tools used in development.  **Customer Responsibility (IaaS)**  The customer is responsible for requiring developers of customer-deployed resources (to include applications, operating systems, databases, and software) to follow a documented development process. The customer control implementation statement should address how the development process: explicitly addresses security requirements; identifies standards and tools used; documents the specific tool options and configurations used; documents, manages, and ensures the integrity of changes to the process and/or tools used in development. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for reviewing the development process, standards, tools, and tool options/configurations as needed to determine if they can satisfy requirements. The customer control implementation statement should address the frequency of the review and the customer-defined security requirements which they are compared to. |

### SA-16 Developer-Provided Training (H)

The organization requires the developer of the information system, system component, or information system service to provide [Assignment: organization-defined training] on the correct use and operation of the implemented security functions, controls, and/or mechanisms.

| SA-16 | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter SA-16: *<FedRAMP Assignment: organization-defined training>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SA-16 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (PaaS)**  The customer is responsible for requiring the developer of customer-deployed resources (to include applications, databases, and software) to provide training. The customer control implementation statement should address the requirement that the developer provide customer-defined training on the correct use and operation of the implemented security functions, controls, and/or mechanisms for the resources provided.  **Customer Responsibility (IaaS)**  The customer is responsible for requiring the developer of customer-deployed resources (to include applications, operating systems, databases, and software) to provide training. The customer control implementation statement should address the requirement that the developer provide customer-defined training on the correct use and operation of the implemented security functions, controls, and/or mechanisms for the resources provided. |

### SA-17 Developer Security Architecture and Design (H)

The organization requires the developer of the information system, system component, or information system service to produce a design specification and security architecture that:

1. Is consistent with and supportive of the organization’s security architecture which is established within and is an integrated part of the organization’s enterprise architecture;
2. Accurately and completely describes the required security functionality, and the allocation of security controls among physical and logical components; and
3. Expresses how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection.

| SA-17 | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SA-17 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (PaaS)**  The customer is responsible for requiring the developer of customer-deployed resources (to include applications, databases, and software) to produce a design specification and security architecture. The customer control implementation statement should address the requirement that the design specification and security architecture is consistent with and supportive of the customer's security architecture.  **Customer Responsibility (IaaS)**  The customer is responsible for requiring the developer of customer-deployed resources (to include applications, operating systems, databases, and software) to produce a design specification and security architecture. The customer control implementation statement should address the requirement that the design specification and security architecture is consistent with and supportive of the customer's security architecture. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for requiring the developer of customer-deployed resources to produce a design specification and security architecture. The customer control implementation statement should address the requirement that the design specification and security architecture accurately and completely describes the required security functionality, and the allocation of security controls among logical resources. |
| Part c | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for requiring the developer of customer-deployed resources to produce a design specification and security architecture. The customer control implementation statement should address the requirement that the design specification and security architecture expresses how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection. |

## System and Communications Protection (SC)

### SC-1 System and Communications Protection Policy and Procedures (H)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A system and communications 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 system and communications protection policy and associated system and communications protection controls; and
2. Reviews and updates the current:
   1. System and communications protection policy [FedRAMP Assignment: at least annually]; and
   2. System and communications protection procedures [FedRAMP Assignment: at least annually or whenever a significant change occurs].

| SC-1 | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter SC-1(a): *<Customer-defined personnel or roles>* | |
| Parameter SC-1(b)(1): *<FedRAMP Assignment: at least annually>* | |
| Parameter SC-1(b)(2): *<FedRAMP Assignment: at least annually or whenever a significant change occurs>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| SC-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for developing, documenting, reviewing, updating, and disseminating system and communications protection policy and procedures for customer-deployed resources. The customer control implementation statement should address the content of the policy (which must include purpose, scope, roles, responsibilities, management commitment, coordination, and compliance), procedures (which must facilitate the implementation of the policies and associated controls), the frequency of review, and the role(s) responsible. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for developing, documenting, reviewing, updating, and disseminating system and communications protection policy and procedures for customer-deployed resources. The customer control implementation statement should address the content of the policy (which must include purpose, scope, roles, responsibilities, management commitment, coordination, and compliance), procedures (which must facilitate the implementation of the policies and associated controls), the frequency of review, and the role(s) responsible. |

### SC-2 Application Partitioning (M) (H)

The information system separates user functionality (including user interface services) from information system management functionality.

| SC-2 | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-2 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for separating system functionality into two separate categories. The customer control implementation statement should address the mechanisms used to separate user functionality from management functionality. |

### SC-3 Security Function Isolation (H)

The information system isolates security functions from nonsecurity functions.

| SC-3 | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-3 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for isolating security functions from nonsecurity functions for customer-deployed resources. The customer control implementation statement should address the mechanisms used to isolate these functions. |

### SC-4 Information in Shared Resources (M) (H)

The information system prevents unauthorized and unintended information transfer via shared system resources.

| SC-4 | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>*; Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-4 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure prevents unauthorized and unintended information transfer by implementing several technical controls for controlling the network, including VLAN segregation, ACLs at all access points into the network, two-factor authentication requirements for all production systems, logging and monitoring at key network devices, and hypervisor isolation for virtual machines. Additionally, no administrative access to the Microsoft Azure network/infrastructure is provided to the customers. Customers can only access the Microsoft Azure services that are publicly available even after authentication. Authentication is performed using customer-specified username and password.  **Customer Responsibility (PaaS)**  The customer is responsible for preventing unauthorized and unintended information transfer between customer-deployed resources (to include applications, databases, and software). The customer control implementation statement should address the mechanisms used to prevent unauthorized and unintended information transfer.  **Customer Responsibility (IaaS)**  The customer is responsible for preventing unauthorized and unintended information transfer between customer-deployed resources (to include applications, operating systems, databases, and software). The customer control implementation statement should address the mechanisms used to prevent unauthorized and unintended information transfer. |

### 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-5 | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>*; Microsoft Azure | |
| Parameter SC-5-1: *<Customer-defined types of denial of service attacks or reference to source for such information>* | |
| Parameter SC-5-2: *<Customer-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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-5 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure has implemented network denial of service protection mechanisms at multiple key points within the system, including the edge router layer and the data center routers. Furthermore, individual Azure services, such as Azure Storage and Azure SQL DB, have additional protections against denial of service attacks targeted at those individual services.  **Customer Responsibility (PaaS)**  The customer is responsible for protecting customer-deployed resources (to include applications, databases, and software) from denial of service (DOS) attacks. The customer control implementation statement should address the customer-defined types of DOS attacks, and the customer-defined security safeguards employed to protect against them.  **Customer Responsibility (IaaS)**  The customer is responsible for protecting customer-deployed resources (to include applications, operating systems, databases, and software) from denial of service (DOS) attacks. The customer control implementation statement should address the customer-defined types of DOS attacks, and the customer-defined security safeguards employed to protect against them. |

### 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-6 | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>*; Microsoft Azure | |
| Parameter SC-6-1: *<Customer-defined resources>* | |
| Parameter SC-6-2: *<Selection (one or more); priority; quota>* | |
| Parameter SC-6-3: *<Customer-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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-6 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure's SDL requires consideration of situations where the system may be threatened by resource overutilization. In these cases, individual Microsoft Azure servers are configured to limit the use of processor and memory resources by process priority. Additionally, clusters of servers (e.g., database clusters) are load-balanced to ensure that no single machine is loaded too heavily. Virtual machine resources are monitored and balanced by the HostOS on each individual physical machine and Azure’s Fabric Controller between physical machines within the environment.  **Customer Responsibility (IaaS/PaaS)**  The customer may be responsible for implementing a subset of resource availability requirements. For example, Microsoft performs resource management on the underlying infrastructure that supports all customer-deployed resources; however, customers may be responsible for performing virtual machine OS-level and/or application-level resource prioritization depending on the customer system design and requirements. The customer control implementation statement should address customer resource availability criteria and how associated resource management is implemented. |

### 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-defined>*; Microsoft Azure | |
| Parameter SC-7(b): 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-7 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure implements boundary protection through the use of controlled devices at the network boundary and at key points within the Microsoft Azure infrastructure. The overarching principle within Microsoft Azure is to allow only connection and communication that is necessary for systems to operate, blocking all other ports, protocols and connections by default. Boundary protection at the edge router network level is inherited from Azure.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for monitoring and controlling communications at and within the boundaries of the customer-deployed system. The customer control implementation statement should address the locations where the monitoring and controlling of traffic occurs. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure's load balancers and public-facing server roles are the only publicly-accessible components. All non-publicly-accessible Microsoft Azure components connect to the load balancers via physically-separate network interfaces on subnets that are logically separated from internal subnets. The hypervisor is isolated from interactions by virtual machines on port 80.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for implementing subnetworks for customer-deployed resources. The customer control implementation statement should address the networks logically separating publicly accessible resources from internal resources. |
| Part c | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure connects to external networks or information systems only through Azure Networking’s managed networks and Azure’s edge routers. The network interfaces provide boundary protection at the edge router network level and are arranged in accordance with organizational security architecture. Additional measures in place to help protect Microsoft Azure information systems from malicious activities include:   * Software load balancers * Non-routable IP addressing * Packet filtering * Host-based firewalls * VLAN isolation * Jump boxes.   **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for managing connections to external networks or systems. The customer control implementation statement should address the managed interfaces, consisting of boundary protection devices arranged in accordance with the customer's security architecture, to which connections to external networks or systems will be restricted. |

#### SC-7 (3) Control Enhancement (M) (H)

The organization limits the number external network connections to the information system.

| SC-7 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>*; Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-7 (3) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure controls and monitors all inbound and outbound traffic through a limited number of network access points at the boundary and at key points within the system. Microsoft Azure leverages the following security mechanisms to limit the number of external network connections to the information system:  Load balancing: limiting inbound access to Microsoft Azure, Microsoft Azure Management Portal, front-end (e.g., FFE, XFE, RDFE), and Customer VM RDP. Each datacenter contains two groups of Jumpboxes behind a load balancer to limit the access points for administration traffic, and customer traffic passes through a load balancer as well. Both entry points are monitored and generate audit logs and alerts in real time.  Jump boxes: control all access to Microsoft Azure, the infrastructure and Customer VMs.  Access of IaaS services: Microsoft Azure (including Microsoft Azure SQL DB) services are only accessible to agency users through the Microsoft Azure provisioning portal and Web Services (REST API) interfaces; two-factor authentication (2FA) is required for both internal (e.g., Microsoft) and external (e.g., Customer).  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for limiting the number of external connections established to the customer-deployed system. The customer control implementation statement should address the number of allowed external connections to customer-deployed resources. |

#### SC-7 (4) Control Enhancement (H)

The organization:

1. Implements a managed interface for each external telecommunication service;
2. Establishes a traffic flow policy for each managed interface;
3. Protects the confidentiality and integrity of the information being transmitted across each interface;
4. Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and
5. Reviews exceptions to the traffic flow policy [FedRAMP Assignment: at least every ninety (90) days or whenever there is a change in the threat environment that warrants a review of the exceptions] and removes exceptions that are no longer supported by an explicit mission/business need.

| SC-7 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: Microsoft Azure | |
| Parameter SC-7(4)(e): *<FedRAMP Assignment: at least every ninety (90) days or whenever there is a change in the threat environment that warrants a review of the exceptions>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-7 (4) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure establishes edge routers as the managed interface for each telecommunication service. Edge routers serve as the first layer of network devices into the Microsoft Azure environment. These devices are managed by the Azure Networking team within Microsoft Azure.  **Customer Responsibility (IaaS/PaaS)**  Customers are not responsible for datacenter operations (to include telecommunications services). All telecommunication services are provided and managed by Microsoft Azure. This control is inherited from Azure. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure Networking establishes routing policies at the edge to only allow the export of 8075 public blocks to Microsoft Azure’s Border Gateway Protocol (BGP) peers. Edge Access Control Lists (ACLs) are applied inbound from all peering interfaces. The policy explicitly filters non “edge protocols” (SQL, RPC, 445, 135-139) from entering the network from untrusted sources.  **Customer Responsibility (IaaS/PaaS)**  Customers are not responsible for datacenter operations (to include telecommunications services). All telecommunication services are provided and managed by Microsoft Azure. This control is inherited from Azure. |
| Part c | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure protects the confidentiality and integrity of information being transmitted, which is documented in SC-8 and SC-9 of the Microsoft Azure SSP.  **Customer Responsibility (IaaS/PaaS)**  Customers are not responsible for datacenter operations (to include telecommunications services). All telecommunication services are provided and managed by Microsoft Azure. This control is inherited from Azure. |
| Part d | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure documents each exception to the traffic flow policy via the security review process with a supporting mission/business need and duration of that need. In the event an exception is needed from the traffic flow policy, a security review (SR) is documented and reviewed by the Online Services Security and Compliance team (OSSC). The request is reviewed by the Security Architecture team who determines if the exception is approved.  **Customer Responsibility (IaaS/PaaS)**  Customers are not responsible for datacenter operations (to include telecommunications services). All telecommunication services are provided and managed by Microsoft Azure. This control is inherited from Azure. |
| Part e | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure documents each exception to the traffic flow policy via the OSSC Policy Exception process with a supporting mission/business need and duration of that need. In the event an exception is needed from the traffic flow policy, a security review (SR) is documented and reviewed by the Online Services Security and Compliance team (OSSC). The request is reviewed by the Security Architecture team who determines if the exception is approved.  All exceptions are reviewed on at least an annual basis. The Azure Networking team removes all traffic flow policy exceptions that are no longer supported by a business need in Microsoft Azure. In the event that the Azure Networking team identifies and reviews a traffic flow policy exception that is no longer needed, they will remove that exception.  Microsoft Azure blocks administrative ports on the internet edge of the environment through the Edge ACL baseline. To detect any authorized changes to the established traffic flow polices on the Microsoft Azure boundary the Microsoft Azure security monitoring team automatically scans the internet boundary of the Azure environment every 4 hours. If a blocked port becomes open, a ticket will be automatically created in the ticketing system and an alert will be created for the Microsoft Azure Security Incident Management (SIM) team to remediate.  Microsoft Azure considers the detection of unauthorized port usage to be a sufficient alternative to performing bi-annual reviews of traffic flow exceptions.  **Customer Responsibility (IaaS/PaaS)**  Customers are not responsible for datacenter operations (to include telecommunications services). All telecommunication services are provided and managed by Microsoft Azure. This control is inherited from Azure. |

#### 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-7 (5) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>*; Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-7 (5) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure’s over-arching principle of network security is deny-by-default and blocks all ports, protocols and connections by default. Microsoft Azure only allows connections and communication that are necessary to operate the system. Connections are managed at the system boundary using Microsoft Azure Networking boundary protection devices. Connections within the boundary are managed using:   * IP Filtering * VFP Filtering (for virtual machines) * Host-based firewalls * Guest firewalls (for virtual machines)   **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for configuring managed network interfaces to deny all traffic by default and permit by exception. The customer control implementation statement should address each type of managed interface throughout the customer-deployed system and describe the method in which each interface deploys a deny all and permit by exception rule. |

#### 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-7 (7) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-7 (7) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for preventing split tunneling for remote devices connecting to the customer-deployed system. The customer control implementation statement should address the methods used for preventing split tunneling at the system as well as the remote device. |

#### 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-7 (8) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter SC-7(8)-1: *<Customer-defined internal communications traffic>* | |
| Parameter SC-7(8)-2: *<Customer-defined 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-7 (8) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for routing customer-defined information through an authenticated proxy to an external network. The customer control implementation statement should address the information which requires routing via proxy as well as the external network that information is routed to. |

#### SC-7 (10) Control Enhancement (H)

The organization prevents the unauthorized exfiltration of information across managed interfaces.

| SC-7 (10) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-7 (10) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for preventing unauthorized exfiltration of information across managed interfaces. The customer control implementation statement should address the mechanisms in place to prevent the unauthorized exfiltration of data. |

#### SC-7 (12) Control Enhancement (H)

The organization implements [FedRAMP Assignment: Host Intrusion Prevention System (HIPS), Host Intrusion Detection System (HIDS), or minimally a host-based firewall] at [Assignment: organization-defined information system components].

| SC-7 (12) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>*; Microsoft Azure | |
| Parameter SC-7(12)-1: *<FedRAMP Assignment: Host Intrusion Prevention System (HIPS), Host Intrusion Detection System (HIDS), or minimally a host-based firewall>* | |
| Parameter SC-7(12)-2: *<Customer-defined 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-7 (12) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (PaaS)**  Microsoft Azure implements this control for the hosts supporting the PaaS environment.  Microsoft Azure implements the following host-based boundary protection mechanisms:   * IP Filtering * VFP Filtering (for virtual machines) * Host-based firewalls * Guest firewalls (for virtual machines)   **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (PaaS)**  Microsoft Azure enforces host-based boundary protection at the PaaS virtual machines associated with the customer’s Azure subscription. As such, this control is inherited from Microsoft Azure.  **Customer Responsibility (IaaS)**  The customer is responsible for implementing host-based boundary protection at customer-deployed virtual machines running customer-controlled operating systems. The customer control implementation statement should address the mechanism and rules associated with the host-based protection**.** |

#### SC-7 (13) Control Enhancement (H)

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 security administration and isolates those tools, mechanisms, and support components from other internal information system components via physically or logically separate subnets.

Guidance: Examples include: information security tools, mechanisms, and support components such as, but not limited to public key infrastructure (PKI), patching infrastructure, cyber defense tools, special purpose gateway, vulnerability tracking systems, internet access points (IAPs); network element and data center administrative/management traffic; demilitarized zones (DMZs), Server farms/computing centers, centralized audit log servers, etc.

| SC-7 (13) | Control Summary Information |
| --- | --- |
| Responsible Role: Microsoft Azure | |
| Parameter SC-7(13): SecurID systems, Security Incident Management systems, Audit Collection systems, Security scanning 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-7 (13) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure has implemented multiple mechanisms for isolating the customer environment, infrastructure components and administrative tools. These mechanisms include:   * VLAN Isolation: isolates Fabric Controller and other devices * VM-Switch/Host OS: isolates root OS from guest VMS and from one another * Storage Accounts: each Storage Account has a unique secret key * Administrative/diagnostic tools, such as FCClient, DEClient, ACIS Portal   In addition, all administrator activity is logged using MDS with tamper-resistant capabilities. Refer to AU-2 for additional details on logging.  **Customer Responsibility (IaaS/PaaS)**  Since customers do not have physical access to any system resources in Azure datacenters, they cannot physically separate customer-deployed resources. Therefore, this control is not applicable. |

#### 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-7 (18) | Control Summary Information |
| --- | --- |
| Responsible Role: Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-7 (18) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure deploys geographically separate and redundant Gateway servers and SSL VPN. When a Gateway system fails, it fails securely and access is restricted to the environment. In order to establish a connection to the Microsoft Azure environment, a user must establish a separate connection to an active Gateway server managed by Microsoft Azure.  Additionally, if Microsoft Azure network devices (including edge routers, access routers, load balancers, aggregation switches, and TORS) fail, the affected circuit becomes disconnected, thereby failing securely. A failure of a Microsoft Azure network device cannot lead to, or cause information external to the system to enter the device, nor can a failure permit unauthorized information release. The built-in redundancy allows Microsoft Azure assets to fail without impacting availability.  **Customer Responsibility (IaaS/PaaS)**  Microsoft Azure manages network boundary devices, which are designed to fail securely. This control is inherited from Microsoft Azure. Note: The customer can implement additional Azure services (e.g., load balancer, application gateway) to support Azure boundary protection mechanisms already in place. |

#### SC-7 (20) Control Enhancement (H)

The information system provides the capability to dynamically isolate/segregate [Assignment: organization-defined information system components] from other components of the system.

| SC-7 (20) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter SC-7 (20): *<Customer-defined 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-7 (20) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for ensuring that the system has the capability to dynamically isolate customer-deployed resources. The customer control implementation statement should address the mechanisms used to dynamically isolate/segregate customer-defined resources from other resources within the system. |

#### SC-7 (21) Control Enhancement (H)

The organization employs boundary protection mechanisms to separate [Assignment: organization-defined information system components] supporting [Assignment: organization-defined mission and/or business functions].

| SC-7 (21) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter SC-7 (21)-1: *<Customer-defined information system components>* | |
| Parameter SC-7 (21)-2: *<Customer-defined mission and/or business 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-7 (21) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for ensuring that the system has the capability to separate customer-deployed resources. The customer control implementation statement should address how the customer employs boundary protection mechanisms to separate customer-defined resources supporting organizational missions and/or business functions. |

### SC-8 Transmission confidentiality and Integrity (M) (H)

The information system protects the [FedRAMP Assignment: confidentiality AND integrity] of transmitted information.

| SC-8 | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>*; Microsoft Azure | |
| Parameter SC-8: *<FedRAMP Assignment: 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-8 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure implements the transmission integrity and confidentiality control by ensuring that cryptography is implemented through a hybrid model. The following is a high-level list of the symmetric and asymmetric keys used for encrypting and protecting confidentiality of data.   * Use AES for symmetric encryption/decryption * Use 128-bit or better symmetric keys * Use RSA for asymmetric encryption/decryption and signatures * Use 2048-bit or better RSA keys * Use SHA-256 or better (SHA-384, SHA-512) for hashing and message-authentication codes   In addition, Microsoft Azure has implemented cryptography in the following ways:  Communications between the Microsoft Azure service offerings and the Microsoft Azure Management Portal are configured to accept FIPS 140-2 validated encryption. The customer is responsible for requiring FIPS 140-2 validated encryption levels on their users’ browsers. The customer would configure this through client configuration settings such as FDCC/USGCB or other configuration on their desktop or mobile device.  Microsoft Azure virtual environment enforces key communications between Microsoft Azure internal components to be protected with self-signed SSL certificates.  Hardware Security Modules used by the KeyVault service employ FIPS 140-2 validated encryption.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for configuring all customer-deployed resources to communicate through FIPS 140-2 validated encryption. The customer control implementation statement should address each type of customer-deployed resource in use and the mechanisms in place on those resources to protect the confidentiality and integrity of the information being transmitted. Note: customers who enforce FDCC/USGCB settings will achieve FIPS 140-2 encryption for data transmitted. |

#### 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-8 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>*; Microsoft Azure | |
| Parameter SC-8 (1)-1: *<FedRAMP Assignment: prevent unauthorized disclosure of information AND detect changes to information>* | |
| Parameter SC-8 (1)-2: *<FedRAMP Assignment: 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-8 (1) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure uses encryption to prevent unauthorized disclosure of information and detect changes to information during transmission. Specifically, Microsoft Azure provides FIPS 140-2 compliant ciphers that include integrity validation for customer connections, interconnected system connections, and remote access connections.  For connections to customers, Microsoft Azure is configured to negotiate FIPS compliant TLS protocols with supported client browsers, though non-FIPS compliant protocols are supported for legacy browser support.  FIPS 140-2 encryption modules used for transmitted information are certified by NIST via certificates 1321, 1333, 1334, 1335, 1336, 1339, 1891, 1892, 1895, 1896, 1897, 1898, and 1899.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for protecting information in transit. The customer control implementation statement should address the cryptographic mechanisms preventing the unauthorized disclosure of and/or detecting changes to customer-controlled information. |

### SC-10 Network Disconnect (H)

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 ten (10) minutes for privileged sessions and no longer than fifteen (15) minutes for user sessions] of inactivity.

| SC-10 | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>*; Microsoft Azure | |
| Parameter SC-10: *<FedRAMP Assignment: no longer than ten (10) minutes for privileged sessions and no longer than fifteen (15) minutes for user 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-10 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure jump boxes disconnect network sessions after 15 minutes of inactivity.  Customers are responsible for implementing portions of this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for implementing a network disconnect for customer-deployed resources. The customer control implementation statement should address the requirement that network connections are terminated at the end of a communication session, and the time period within which network connections are terminated due to 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-defined>*; Microsoft Azure | |
| Parameter SC-12: *<Customer-defined requirements for key generation, distribution, storage, access, and destruction>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-12 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure leverages the cryptographic capabilities that are directly a part of the Windows operating system for certificates and authentication mechanisms such as Kerberos v5. These cryptographic modules have been certified by NIST as being FIPS 140-2 compliant. Relevant NIST certificate numbers are: 1321, 1333, 1334, 1335, 1336, 1339, 1891, 1892, 1895, 1896, 1897, 1898, and 1899. Additionally, the Thales nShield Hardware Security Modules used by KeyVault employ cryptographic modules certified by NIST as being FIPS 140-2 compliant; relevant NIST certificate numbers are: 2148, 2149. Finally, the Ubuntu Linux servers used by MFA employ NIST-certified FIPS 140-2 compliant cryptographic modules; the relevant NIST certificate number is 1747. Any time cryptographic capabilities are employed to protect the confidentiality, integrity, or availability of data within Azure, the modules and ciphers (which include AES, and RSA) 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  New SSL certificates are generated as part of the deployment of a new service. The service operations team uses an internal Microsoft tool (Identity and Access Management - SSL Authorization) to generate new SSL certificates, which are then deployed into the service following standard processes for certificate management.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for managing cryptographic keys used within customer-deployed resources. The customer control implementation statement should address the required cryptography employed in accordance with customer-defined requirements for key generation, distribution, storage, access, and destruction. |

#### SC-12 (1) Control Enhancement (H)

The organization maintains availability of information in the event of the loss of cryptographic keys by users.

| SC-12 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-12 (1) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for maintaining the availability of information in the event of the loss of cryptographic keys by users. The customer control implementation statement should address the mechanisms in place to maintain availability (e.g., using Azure Key Vault to manage secrets). |

#### 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-defined>* | |
| Parameter SC-12 (2): *<FedRAMP Selection: NIST FIPS-compliant>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-12 (2) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for producing, controlling, and distributing symmetric cryptographic keys (if they are used within customer-deployed resources) using compliant key management technology and processes. The customer control implementation statement should address the mechanisms used for NIST FIPS-compliant and/or NSA-approved key management. |

#### 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: *<Customer-defined>* | |
| Parameter SC-12 (3): *<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>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-12 (3) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for producing, controlling, and distributing asymmetric cryptographic keys (if they are used within customer-deployed resources). The customer control implementation statement should address the requirement that asymmetric cryptographic keys are managed using one or more of the following: 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-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-defined>*; Microsoft Azure | |
| Parameter SC-13: *<FedRAMP Assignment: FIPS-validated or NSA-approved cryptography>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-13 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure service teams use encryption mechanisms and techniques that follow the requirements and restrictions outlined in the Microsoft Azure Cryptographic Control SOP. Service data and information are handled in accordance with the requirements and restrictions specified in the Microsoft Azure Asset Management standard when cryptography is used. The Microsoft Azure Asset Management document establishes the mandatory minimum requirements for Microsoft Azure asset ownership, classification, and protection.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for implementing customer-defined cryptography within customer-deployed resources. The customer control implementation statement should address the types of cryptography used and how they are used in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. |

### 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 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 | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter SC-15(a): *<FedRAMP Assignment: no exceptions>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-15 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for prohibiting remote activation of any collaborative computing devices within or controlled from customer-deployed resources. The customer control implementation statement should address the mechanisms preventing the activation of collaborative computing devices and customer-defined exceptions where remote activation is allowed (if any).  FedRAMP Requirement: The customer is responsible for providing ease of use functionality to disable any collaborative computing devices within customer-deployed resources. The customer control implementation statement should address the mechanism in place for disabling collaborative computing devices. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for providing a notification when physically presenting at a collaborative device. The customer control implementation statement should address the mechanism which explicitly identifies any customer deployed resource when it is being used as a collaborative device. |

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: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-15 What is the solution and how is it implemented? | |
| --- | --- |
| Req. 1 | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for prohibiting remote activation of any collaborative computing devices within or controlled from customer-deployed resources. The customer control implementation statement should address the mechanisms preventing the activation of collaborative computing devices and customer-defined exceptions where remote activation is allowed (if any).  FedRAMP Requirement: The customer is responsible for providing ease of use functionality to disable any collaborative computing devices within customer-deployed resources. The customer control implementation statement should address the mechanism in place for disabling collaborative computing devices. |

### 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-defined>;* Microsoft Azure | |
| Parameter SC-17: *<Customer-defined certificate 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-17 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft’s corporate Public Key Infrastructure (PKI) has been established to provide a variety of digital certificate services to support operations for Microsoft Azure 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.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for defining and enforcing a policy for issuing public key certificates. The customer control implementation statement should address the requirement that public key certificates are issued under a customer-defined policy or obtained from an approved service provider. |

### 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: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-18 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for defining acceptable and unacceptable mobile code technologies. The customer control implementation statement should address the types of mobile code allowed in customer-deployed resources. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for establishing code restrictions and guidance. The customer control implementation statement should address how the customer establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies. |
| Part c | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for authorizing, monitoring, and controlling the use of mobile code within customer-deployed resources. The customer control implementation statement should address how the customer authorizes, monitors and controls the use of 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-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-19 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for managing Voice over Internet Protocol (VoIP) technologies. The customer control implementation statement should address the usage restrictions and implementation guidance for VoIP technologies based on the potential to cause damage to customer-deployed resources, if used maliciously. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for managing Voice over Internet Protocol (VoIP) technologies. The customer control implementation statement should address how the customer authorizes, monitors and controls the use of VoIP within customer-deployed resources. |

### 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
2. 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: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-20 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for a secure name and address resolution service. The customer control implementation statement should address the mechanisms in place for providing data origin authentication and integrity verification as well as authoritative name resolution data in response to name and address resolution queries. Note: this control is only applicable to the customer if hosting DNS and resolving .gov domains. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for a secure name and address resolution service. The customer control implementation statement should address the customer-deployed system's ability to provide the security status of child zones, in order to verify chain of trust among parent and child domains. Note: this control is only applicable to the customer if hosting DNS and resolving .gov domains. |

### 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: *<Customer-defined>*; Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-21 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure uses three types of DNS servers:  System DNS servers – these act as non-authoritative sources for DNS requests only from clients hosted inside Microsoft Azure. A client makes a DNS query to a system DNS server; the system DNS server in turn queries an authoritative source outside the system. System DNS servers do not support the DNSSEC protocol. This control requires system DNS servers, when requested by clients, to perform origin/integrity verification of the response provided by authoritative sources. The control assumes that the client makes a DNS query of a system DNS server and that the DNS server must then query an authoritative source outside the system. The risk that the external authoritative source has been compromised is mitigated by the origin/integrity verification.  Microsoft Azure internal DNS servers resolve DNS queries from Microsoft Azure servers. Microsoft Azure servers do not request origin/integrity verification of the DNS query; instead origin/integrity is assured via other means such as the communications channel using TLS, as discussed in SC-8 and SC-11.  Microsoft Azure DNS's production servers act as authoritative sources for DNS requests from external clients for various Microsoft Azure domains and will not respond to any DNS queries against zones for which they are not the authority.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for configuring customer-deployed resources to request and perform data origin authentication and data integrity verification on name/address resolution responses received from authoritative sources. The customer control implementation statement should address the DNS implementation in place for validating and authenticating DNS requests. |

### 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: *<Customer-defined>*; Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-22 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure DNS shared services, as reflected in the boundary, provide name and address resolution. Fault tolerance is built into the service through redundancy at multiple levels (multiple DNS server clusters and multiple servers per cluster) and deployment at multiple Microsoft Azure datacenter facilities which are geographically separated. Internal name resolution is handled by separate servers than external name resolution. DNS shared services also leverages network controls to restrict type of hosts that can access an authoritative DNS server in a particular role.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for ensuring that the systems providing address resolution services for customer-deployed resources are fault-tolerant and implement internal/external role separation. The customer control implementation statement should address the systems providing name/address resolution, and how they are fault-tolerant and implement internal/external role separation. Note: if customers configure their Domain Name Server (DNS) settings to use Microsoft Azure servers, Microsoft Azure DNS can support fault tolerance. |

### SC-23 Session Authenticity (M) (H)

The information system protects the authenticity of communications sessions.

| SC-23 | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>*; Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-23 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure uses digital certificates to establish the identity of Jumpboxes as the access point to the Microsoft Azure 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 is resistant to man in the middle attacks.  All communications between Microsoft Azure internal components that transfer confidential information are protected using TLS.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for protecting the authenticity of communications sessions involving customer-deployed resources. The customer control implementation statement should address how the customer enforces authenticity protection (e.g., guarding against man-in-the-middle attacks, session hijacking, and the insertion of false information into sessions). |

#### SC-23 (1) Enhancement (H)

The information system invalidates session identifiers upon user logout or other session termination.

| SC-23 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-23 (1) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for invalidating session identifiers at logout. The customer control implementation statement should address the mechanisms in place to ensure that session identifiers are invalidated upon user log out or other session termination. |

### SC-24 Fail in Known State (H)

The information system fails to a [Assignment: organization-defined known-state] for [Assignment: organization-defined types of failures] preserving [Assignment: organization-defined system state information] in failure.

| SC-24 | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter SC-24-1: *<Customer-defined known-state>* | |
| Parameter SC-24-2: *<Customer-defined types of failures>* | |
| Parameter SC-24-3: *<Customer-defined system state 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-24 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for ensuring customer-deployed resources fail in a known-state. The customer control implementation statement should address the customer-defined known-state the system fails to, the types of failures this applies to, as well as how it preserves the system state information in failure. |

### 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: *<Customer-defined>*; Microsoft Azure | |
| Parameter SC-28-1: *<FedRAMP Selection: confidentiality AND integrity>* | |
| Parameter SC-28-2: *<Customer-defined information at rest>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-28 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure protects information at rest by applying information-handling procedures. Assets must be protected according to the standards appropriate for their defined asset class. Microsoft’s Online Services has devised a set of minimum required protection standards for each asset class in order to appropriately protect the confidentiality, integrity, and availability of each asset. These minimum standards are defined in Appendix A of the Microsoft’s Online Services Asset Classification and Protection Standards. Data must be classified according to LCA data classifications and associated retentions.  Protections for information at rest are outlined in, but not limited to, the categories below:  Access Control – Logical access to protected data at rest is controlled at various levels through technical means. Access to servers where information is stored is restricted through Active Directory security group membership in the domain where the server resides. Security groups that restrict access to information at rest are configured to allow the least privilege possible to complete tasks. Any Microsoft administrator needing access must follow account creation or modification procedures as outlined in AC-2.  Technical means also create logical access control at the network layer. Router and firewall ACLs prevent servers that store data at rest from being exposed outside of the environment.  Physical Access Controls – The Microsoft Azure Datacenter team maintains controls over physical access to the Datacenter. The server room environments have multiple access levels regulated with least privilege.  For each block written to Azure Storage accounts, a compressed and uncompressed CRC is used to identify corrupted data. Azure Storage checks the CRC after every major handoff of the data. In addition, a background job periodically runs on the extant nodes checking the data checksum to find corrupted data.  In addition to these mitigating controls, Azure DNS uses both Microsoft Azure Tape Backup Services and System Center Data Protection Manager. All data that is backed up is encrypted prior to writing to tape or disk, which protects both the confidentiality and the integrity of the backed-up data.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for protecting customer-controlled information at rest. The customer control implementation statement should address the customer-defined information which requires protection of its confidentiality and/or integrity. |

#### SC-28 (1) Control Enhancement (H)

The information system implements cryptographic mechanisms to prevent unauthorized disclosure and modification of [Assignment: organization-defined information] on [FedRAMP Assignment: all information system components storing customer data deemed sensitive]

| SC-28 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>*; Microsoft Azure | |
| Parameter SC-28(1)-1: *<Customer-defined information>* | |
| Parameter SC-28(1)-2: *<FedRAMP Assignment: all information system components storing customer data deemed sensitive>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-28 (1) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure protects the confidentiality and integrity of customer data on Microsoft Azure servers using the information-handling procedures outlined in SC-28.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for protecting customer-controlled information at rest. The customer control implementation statement should address the customer-controlled information on customer-defined resources which require protection from unauthorized disclosure and modification. |

### 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: *<Customer-defined>*; Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-39 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure implements this control for the operating systems supporting the PaaS environment.  Microsoft Azure servers run Windows Server 2008 or 2012, or Ubuntu Linux. In either case, these operating systems maintain separate execution domains 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>  **Customer Responsibility (PaaS)**  Microsoft Azure implements separate execution domains for the Windows operating system leveraged by PaaS customers. Customers inherit this control for PaaS resources implemented on Microsoft Azure.  **Customer Responsibility (IaaS)**  The customer is responsible for maintaining separate execution domains for running processes. The customer control implementation statement should address the mechanisms in place separating execution domains (most modern operating systems, if deployed without tampering, implement this function). |

## System and Information Integrity (SI)

### SI-1 System and Information Integrity Policy and Procedures (H)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A system and information integrity 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 information integrity policy and associated system and information integrity controls; and
2. Reviews and updates the current:
   1. System and information integrity policy [FedRAMP Assignment: at least annually]; and
   2. System and information integrity procedures [FedRAMP Assignment: at least annually or whenever a significant change occurs].

| SI-1 | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter SI-1(a): *<Customer-defined personnel or roles>* | |
| Parameter SI-1(b)(1): *<FedRAMP Assignment: at least annually>* | |
| Parameter SI-1(b)(2): *<*FedRAMP Assignment: at least annually or whenever a significant change occurs> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| SI-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for developing, documenting, reviewing, updating, and disseminating system and information integrity policy and procedures for customer-deployed resources. The customer control implementation statement should address the content of the policy (which must include purpose, scope, roles, responsibilities, management commitment, coordination, and compliance), procedures (which must facilitate the implementation of the policies and associated controls), the frequency of review, and the role(s) responsible. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for developing, documenting, reviewing, updating, and disseminating system and information integrity policy and procedures for customer-deployed resources. The customer control implementation statement should address the content of the policy (which must include purpose, scope, roles, responsibilities, management commitment, coordination, and compliance), procedures (which must facilitate the implementation of the policies and associated controls), the frequency of review, and the role(s) responsible. |

### 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-defined>*; Microsoft Azure | |
| Parameter SI-2(c): *<FedRAMP Assignment: thirty 30 days of release of updates>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (PaaS)**  Microsoft Azure implements this control for the operating systems supporting the PaaS environment.  Each VM image is deployed with the latest available version of the OS. Microsoft Azure identifies, reports, and corrects information system flaws through vulnerability management, incident response management, and patch/configuration management processes. The Microsoft Azure Incident Management Program assists with identifying and reporting of information system flaws. Microsoft Azure receives vulnerability-related data from multiple sources of information which include: Microsoft Security Resource Center (MSRC), vendor websites, other third-party services (e.g., Internet Security Systems) and internal/external vulnerability scanning of services. Microsoft Azure Security will determine which updates are applicable within the Microsoft Azure environment. Potential changes are tested in advance. Patching schedules are defined by Microsoft Azure Security as follows:  • 30 days for high vulnerabilities  • 90 days for medium/moderate vulnerabilities  • 180 days for low vulnerabilities.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (PaaS)**  The customer is responsible for flaw remediation on customer-deployed resources (to include applications, databases, and software). The customer control implementation statement should address the identification of flaws and how they are reported and corrected.  **Customer Responsibility (IaaS)**  The customer is responsible for flaw remediation on customer-deployed resources (to include applications, operating systems, databases, and software). The customer control implementation statement should address the identification of flaws and how they are reported and corrected. |
| Part b | **Microsoft Azure (PaaS)**  Microsoft Azure implements this control for the operating systems supporting the PaaS environment.  Microsoft Azure tests potential software and firmware changes prior to deployment, either in a separate test environment, or by removing a server from production, making changes, testing, and returning the server to production upon successful completion.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing is control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for testing updates related to flaw remediation for effectiveness and potential side effects prior to installation on customer-deployed resources. The customer control implementation statement should address the testing process of resource updates prior to installation. |
| Part c | **Microsoft Azure (PaaS)**  Microsoft Azure implements this control for the operating systems supporting the PaaS environment.  Each VM image is deployed with the latest available version of the OS. Microsoft Azure installs security-relevant software and firmware updates within 30 days for updates associated with high risk vulnerabilities and 90 days for updates associated with medium/moderate risk vulnerabilities.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing is control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for installing security-relevant software updates to customer-deployed resources. The customer control implementation statement should address the time period within which security-relevant updates are installed after the release of the update. |
| Part d | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing is control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for including flaw remediation in configuration management. The customer control implementation statement should address the incorporation of flaw remediation activities into the organization's configuration management process. |

#### SI-2 (1) Control Enhancement (H)

The organization centrally manages the flaw remediation process.

| SI-2 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-2 (1) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing is control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for managing flaw remediation. The customer control implementation statement should address the mechanisms used to centrally manage the flaw remediation process (e.g., planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed flaw remediation security 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-2 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter SI-2 (2): *<FedRAMP Assignment: 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-2 (2) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing is control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for employing automated mechanisms to determine flaw remediation status. The customer control implementation statement should address the mechanisms employed to determine the state of customer-deployed resources with regard to flaw remediation, and the customer-defined frequency by which this occurs. |

#### 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: *<Customer-defined>* | |
| Parameter SI-2(3)(b): *<Customer-defined benchmarks>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-2 (3) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing is control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for remediating flaws within customer-deployed resources. The customer control implementation statement should address the mechanisms in place to measure the time between flaw identification and flaw remediation. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing is control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for remediating flaws within customer-deployed resources. The customer control implementation statement should address the establishment of customer-defined benchmarks for taking corrective actions. |

### SI-3 Malicious Code Protection (H)

The organization:

1. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code;
2. Updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures;
3. Configures malicious code protection mechanisms to:
   1. 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
   2. [FedRAMP Assignment: to include blocking and quarantining malicious code and alerting administrator or defined security personnel near-real-time] in response to malicious code detection; and
4. 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-defined>* | |
| Parameter SI-3(c)(1)-1: *<FedRAMP Assignment: at least weekly>* | |
| Parameter SI-3(c)(1)-2: *<FedRAMP Assignment: to include endpoints>* | |
| Parameter SI-3(c)(2): *<FedRAMP Assignment: to include blocking and quarantining malicious code and alerting administrator or defined security personnel near-real-time>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing is control.  **Customer Responsibility (PaaS)**  The customer is responsible for protecting customer-deployed resources (to include applications, databases, and software) against malicious code. The customer control implementation statement should address the use of code protection mechanisms at entry and exit points to detect and eradicate malicious code (e.g., viruses, malware, rootkits, worms, and scripts).  **Customer Responsibility (IaaS)**  The customer is responsible for protecting customer-deployed resources (to include applications, operating systems, databases, and software) against malicious code. The customer control implementation statement should address the use of code protection mechanisms at entry and exit points to detect and eradicate malicious code (e.g., viruses, malware, rootkits, worms, and scripts). |
| Part b | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing is control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for protecting customer-deployed resources against malicious code. The customer control implementation statement should address the requirement that malicious code protection mechanisms are updated when new releases are available, in accordance with organizational configuration management policy and procedures. |
| Part c | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing is control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for protecting customer-deployed resources against malicious code. The customer control implementation statement should address the configuration of malicious code protection mechanisms to: perform periodic scans at a customer-defined frequency and real-time scans of files from external sources at endpoint and/or network entry/exit points as the files are downloaded, opened, or executed in accordance with organizational security policy; block malicious code, quarantine malicious code, and/or send an alert to an administrator; and take any customer-defined action(s) in response to malicious code detection. |
| Part d | **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing is control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for protecting against malicious code. The customer control implementation statement should address the receipt of false positives during malicious code detection and eradication, and the resulting potential impact on the availability of customer-deployed resources. |

#### SI-3 (1) Control Enhancement (M) (H)

The organization centrally manages malicious code protection mechanisms.

| SI-3 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-3 (1) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing is control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for managing malicious code protection. The customer control implementation statement should address the mechanisms used to centrally manage malicious code protection mechanisms. |

#### SI-3 (2) Control Enhancement (M) (H)

The information system automatically updates malicious code protection mechanisms.

| SI-3 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-3 (2) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing is control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for managing malicious code protection. The customer control implementation statement should address the requirement to automatically update malicious code protection mechanisms. |

#### SI-3 (7) Control Enhancement (M) (H)

The information system implements nonsignature-based malicious code detection mechanisms.

| SI-3 (7) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-3 (7) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing is control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for managing malicious code protection. The customer control implementation statement should address the implementation of a nonsignature-based detection mechanism (e.g., heuristics to detect, analyze and describe the characteristics or behavior of malicious code and provide safeguards against malicious code for which signatures do not yet exist or existing signatures may not be effective). |

### 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
   2. Unauthorized local, network, and remote connections;
2. Identifies unauthorized use of the information system through [Assignment: organization-defined techniques and methods];
3. 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;
4. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;
5. 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;
6. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and
7. 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: *<Customer-defined>*; Microsoft Azure | |
| Parameter SI-4(a)(1): *<Customer-defined monitoring objectives>* | |
| Parameter SI-4(b): *<Customer-defined techniques and methods>* | |
| Parameter SI-4(g)-1: *<Customer-defined information system monitoring information>* | |
| Parameter SI-4(g)-2: *<Customer-defined personnel or roles>* | |
| Parameter SI-4(g)-3: *<Customer-defined frequency>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure implements portions of this control for IaaS and PaaS customers.  Microsoft Azure systems in Microsoft Azure Virtual Environment  Service teams have deployed active monitoring solutions that generate alerts and audit logs. All service teams upload their logs to MDS, where they are aggregated and processed. Reports are generated using SLAM. SLAM assists in identifying normal usage of the system and deviations from that normal range. SLAM 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 violation of the Microsoft Azure Security Policy must be immediately brought to the attention of Microsoft Azure Security.  Microsoft Azure Servers  Azure Servers environment use a similar implementation, managed by OSSC SIM.  Local connections are disallowed by policy within Microsoft Azure. No personnel have local access. Microsoft Azure performs network monitoring and detection of unauthorized connections in accordance with their security policy. Remote authentication failures are logged and stored within MDS and the central log repository used by OSSC (for bare metal servers). For further information, please see AC-17 and AC-7.  **Customer Responsibility (PaaS)**  The customer is responsible for monitoring customer-deployed resources (to include applications, databases, and software). The customer control implementation statement should address the use of monitoring to detect: attacks and indicators of potential attacks in accordance with customer-defined monitoring objectives; and unauthorized local, network, and remote connections.  **Customer Responsibility (IaaS)**  The customer is responsible for monitoring customer-deployed resources (to include applications, operating systems, databases, and software). The customer control implementation statement should address the use of monitoring to detect: attacks and indicators of potential attacks in accordance with customer-defined monitoring objectives; and unauthorized local, network, and remote connections. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure implements portions of this control for IaaS and PaaS customers.  Audit logs are uploaded to MDS and reports are generated using SLAM. SLAM assists in identifying normal usage of the system and deviations from that normal range. SLAM uses heuristics to identify unauthorized use of the operating system. Unusual activity is flagged for further review. Any log event that indicates a potential violation of the Microsoft Azure Security Policy must be immediately brought to the attention of Microsoft Azure Security.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for monitoring customer-deployed resources. The customer control implementation statement should address the identification of unauthorized use through customer-defined techniques and methods. |
| Part c | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure implements portions of this control for IaaS and PaaS customers.  All servers act as monitoring devices and are configured to log all security-relevant events. Microsoft Azure monitors all hosts in the environment. Suspicious events generate alarms and notifications to service team staff and appropriate contingent staff. Logs are aggregated in MDS and reports are generated using SLAM. Microsoft Azure servers are configured to upload their logs to a central repository managed by OSSC. These logs are aggregated and reports are generated by the OSSC SIM team.  All servers are configured to log all exceptions and security-relevant events. Microsoft Azure has determined that there is no need for ad-hoc deployment of monitoring devices.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for monitoring customer-deployed resources. The customer control implementation statement should address the deployment of monitoring devices: strategically to collect customer-defined essential information; and at ad hoc locations to track specific types of transactions of interest to the organization. |
| Part d | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure implements portions of this control for IaaS and PaaS customers.  All servers upload logs to MDS for aggregation and analysis. Access to MDS is restricted as specified in the AU family of controls, specifically AU-9.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for monitoring customer-deployed resources. The customer control implementation statement should address the protection of intrusion-monitoring tool information from unauthorized access, modification, and deletion. |
| Part e | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure implements portions of this control for IaaS and PaaS customers.  Microsoft Azure Security notifies service teams if a change in the level of monitoring is necessary due to indications of increased risk, and service teams adjust monitoring accordingly. Additionally, SLAM heuristics are tailored to look for specific threats based on the nature of the risk to organizational operations and assets.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for monitoring customer-deployed resources. The customer control implementation statement should address the heightening of monitoring activity whenever there is an indication of increased risk to customer operations, assets, and individuals; other organizations; or the Nation based on law enforcement information; intelligence information, or other credible sources of information. |
| Part f | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure implements portions of this control for IaaS and PaaS customers.  Microsoft Azure Security and OSSC SIM, in consultation with Legal and Corporate affairs (LCA), 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 Microsoft Azure services. To fully comply with applicable regulations, the service teams follow defined requirements for event collection and notification processes.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for monitoring customer-deployed resources. The customer control implementation statement should address the requirement that the customer obtains legal opinion with regard to system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations. |
| Part g | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure implements portions of this control for IaaS and PaaS customers.  All systems upload logs to MDS for aggregation and analysis. Reports are generated from this data using SLAM as described AU-6 and AU-7. These reports are available daily and as needed.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for monitoring customer-deployed resources. The customer control implementation statement should address the requirement that the customer provides selected monitoring information to customer-defined personnel/roles as needed and/or at the required frequency. |

#### 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-4 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>*; Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-4 (1) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure implements portions of this control for IaaS and PaaS customers.  Microsoft Azure virtual hosts upload logs to MDS for aggregation and analysis. Microsoft Azure bare metal servers upload logs to a central repository managed by OSSC SIM. Consolidated reports are generated from this data by Microsoft Azure Security and OSSC SIM as described AU-6 and AU-7, and cover system-wide intrusion detections.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for monitoring customer-deployed resources. The customer control implementation statement should address the connection and configuration of individual intrusion detection tools into a system-wide intrusion detection system. |

#### SI-4 (2) Control Enhancement (M) (H)

The organization employs automated tools to support near real-time analysis of events.

| SI-4 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-responsibility>*; Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-4 (2) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure implements portions of this control for IaaS and PaaS customers.  Microsoft Azure systems in Microsoft Azure Virtual Environment  ASM is implemented to support real-time analysis of events within the Microsoft Azure virtual environment. ASM functionality can be broadly categorized as belonging to these categories: data collection, data analysis, and reporting. Data collection is primarily accomplished via a MA listener. MA gathers monitoring and diagnostic log information throughout the Microsoft Azure operating environment. It pushes a digested subset of information into Microsoft Azure MDS for analysis. Data analysis and reporting is accomplished using the monitoring platform filter and reporting functionality, also known as Windows AIMS. For additional information on ASM and AIMS, refer to the AU family of controls.  Microsoft Azure Servers  Microsoft Azure servers are configured to send their logs to a centralized location managed by OSSC SIM, where events are analyzed in near real time.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for monitoring customer-deployed resources. The customer control implementation statement should address the automated mechanisms used to support near real-time analysis of events. |

#### 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-4 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>*; Microsoft Azure | |
| Parameter SI-4(4): *<FedRAMP Assignment: 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-4 (4) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure implements portions of this control for IaaS and PaaS customers.  Microsoft Azure systems in Microsoft Azure Virtual Environment  Microsoft Azure inbound and outbound communications are monitored continually using their centralized monitoring, correlation, and analysis systems that manage the large amount of information generated by devices within the environment. MDS provides automated logging and alerting capabilities by utilizing MAs throughout the system and Microsoft Azure AIMS to generate alerts. For additional information on auditing and monitoring, refer to the AU family of controls.  Microsoft Azure Servers  Microsoft Azure continually monitors inbound and outbound communications for unusual or unauthorized activities or conditions for physical servers and any Microsoft Azure network devices.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for monitoring customer-deployed resources. The customer control implementation statement should address how the system monitors inbound and outbound communications traffic at the customer-defined frequency for unusual or unauthorized activities/conditions. |

#### 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-4 (5) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>*; Microsoft Azure | |
| Parameter SI-4(5)-1: *<Customer-defined personnel or roles>* | |
| Parameter SI-4(5)-2: *<Customer-defined compromise indicators>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-4 (5) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure implements portions of this control for IaaS and PaaS customers.  Microsoft Azure Security has defined requirements for active monitoring. Service teams configure active monitoring tools in accordance with these requirements. Active monitoring tools include the Monitoring Agent (MA) and System Center Operations Manager (SCOM), which are configured to provide real time alerts to Service Engineer Operations personnel in situations that require immediate action. The indications of compromise or potential compromise are documented in the Microsoft Azure Incident Response Plan.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for providing monitoring alerts for customer-deployed resources. The customer control implementation statement should address the mechanisms used to alert customer-defined personnel/roles when specified indications of compromise or potential compromise occur. |

#### SI-4 (11) Control Enhancement (H)

The organization analyzes outbound communications traffic at the external boundary of the information system and selected [Assignment: organization-defined interior points within the system (e.g., subnetworks, subsystems)] to discover anomalies.

| SI-4 (11) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter SI-4 (11): *<Customer-defined interior points within the system (e.g., subnetworks, subsystems)>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-4 (11) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for analyzing communications traffic anomalies for customer-deployed resources. The customer control implementation statement should address the analysis of outbound communications traffic at the external boundary and at customer-defined interior points within the system to discover anomalies. |

#### 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-4 (14) | Control Summary Information |
| --- | --- |
| Responsible Role: Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-4 (14) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure regularly monitors for rogue wireless signals on a quarterly basis as discussed in AC-18. Microsoft Azure implements this control on behalf of both PaaS and IaaS customers.  **Customer Responsibility (IaaS/PaaS)**  Microsoft Azure is responsible for all datacenter operational security. Microsoft Azure is responsible for an intrusion detection system identifying rogue wireless devices. This control can be inherited from Microsoft Azure. |

#### SI-4 (16) Control Enhancement (M) (H)

The organization correlates information from monitoring tools employed throughout the information system.

| SI-4 (16) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>*; Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-4 (16) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure implements portions of this control for IaaS and PaaS customers.  All systems upload logs to MDS or the OSSC log repository for aggregation and analysis. Reports are generated from this data as described AU-6 and AU-7, and cover system-wide intrusion detections.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for correlating monitoring information. The customer control implementation statement should address the process for correlating information gathered from customer-deployed monitoring tools. |

#### SI-4 (18) Control Enhancement (H)

The organization analyzes outbound communications traffic at the external boundary of the information system (i.e., system perimeter) and at [Assignment: organization-defined interior points within the system (e.g., subnetworks, subsystems)] to detect covert exfiltration of information.

| SI-4 (18) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter SI-4 (18): *<Customer-defined interior points within the system (e.g., subnetworks, subsystems)>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-4 (18) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for analyzing communications traffic for customer-deployed resources. The customer control implementation statement should address the analysis of outbound communications traffic at the external boundary and at customer-defined interior points within the system to detect covert exfiltration of information. |

#### SI-4 (19) Control Enhancement (H)

The organization implements [Assignment: organization-defined additional monitoring] of individuals who have been identified by [Assignment: organization-defined sources] as posing an increased level of risk.

| SI-4 (19) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter SI-4 (19)-1: *<Customer-defined additional monitoring>* | |
| Parameter SI-4 (19)-2: *<Customer-defined sources>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-4 (19) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for monitoring individuals who pose a greater risk. The customer control implementation statement should address the customer-defined additional mechanisms used to monitor individuals who have been identified by customer-defined sources as posing an elevated level of risk. |

#### SI-4 (20) Control Enhancement (H)

The organization implements [Assignment: organization-defined additional monitoring] of privileged users.

| SI-4 (20) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter SI-4 (20)-1: *<Customer-defined additional monitoring>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-4 (20) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for monitoring privileged users. The customer control implementation statement should address the customer-defined mechanisms used to monitor privileged users. |

#### SI-4 (22) Control Enhancement (H)

The information system detects network services that have not been authorized or approved by [Assignment: organization-defined authorization or approval processes] and [Selection (one or more): audits; alerts [Assignment: organization-defined personnel or roles]].

| SI-4 (22) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter SI-4 (22)-1: *<Customer-defined authorization or approval processes>* | |
| Parameter SI-4 (22)-2: *<Customer-defined personnel or roles>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-4 (22) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for detecting unauthorized network services. The customer control implementation statement should address the mechanisms used to: detect network services that have not been authorized or approved by customer-defined processes; and audit and/or alert customer-defined personnel/roles. |

#### 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-4 (23) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>*; Microsoft Azure | |
| Parameter SI-4(23)-1: *<Customer-defined host based monitoring mechanisms>*; Windows event logging | |
| Parameter SI-4(23)-2: *<Customer-defined information system components>*; 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-4 (23) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (PaaS)**  Microsoft Azure implements portions of this control for IaaS and PaaS customers.  All hosts within Microsoft Azure have Windows Event Logging enabled. If this functionality is turned off or unsuccessful, an alert will be generated through MDS or OSSC monitoring and the alert will be investigated as a security incident.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (PaaS)**  Microsoft Azure implements host-based monitoring for PaaS resources. Customers inherit this control for PaaS resources implemented on Microsoft Azure.  **Customer Responsibility (IaaS)**  The customer is responsible for implementing host-based monitoring for customer-deployed resources. The customer control implementation statement should address the customer-defined host-based monitoring mechanisms and which resources they are implemented on. |

#### SI-4 (24) Control Enhancement (H)

The information system discovers, collects, distributes, and uses indicators of compromise.

| SI-4 (24) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-4 (24) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for discovering, collecting, distributing, and using indicators of compromise to customer-deployed resources. The customer control implementation statement should address the process for discovering, collecting, distributing, and using indicators of compromise. |

### 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: *<Customer-defined>*; Microsoft Azure | |
| Parameter SI-5(a): *<FedRAMP Assignment: to include US-CERT>* | |
| Parameter SI-5(c): *<FedRAMP Assignment: to include system security personnel and administrators with configuration/patch-management 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (PaaS)**  Microsoft Azure implements this control for the operating systems supporting the PaaS environment.  For all asset types, Microsoft Azure receives information system security alerts, advisories, and directives from a number of external communications including US-CERT and USCYBERCOM.  Customers can report security incidents at any time through the Microsoft Azure Management Portal or via a 24x7 dedicated phone line that is available.  Microsoft’s OSSC SIM team notifies partner teams of security incidents which occur within the physical environment (i.e. data centers and boundary network devices).  MSRC notifies partner teams around the latest security patches for Microsoft’s software platforms. MSRC publishes Security Bulletins and associated patches on the second Tuesday of every month except when MSRC determines that an out of band patch is required for addressing zero day vulnerabilities.  Working with MSRC and OSSC-SIM, external parties such as Law Enforcement, ISPs, and other partners can identify security issues. For example, GIAIS utilizes the MSRC Alliance to feed security concerns to Microsoft’s Online Services, including Microsoft Azure.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (PaaS)**  The customer is responsible for managing security alerts, advisories and directives for customer-deployed resources (to include applications, databases, and software). The customer control implementation statement should address the requirement that the customer receives system security alerts, advisories, and directives from customer-defined external organizations on an ongoing basis. Note: Microsoft Azure is responsible for receiving relevant alerts related to the operating system for PaaS resources. The customer will still be responsible for receiving alerts for all other customer-deployed resources.  **Customer Responsibility (IaaS)**  The customer is responsible for managing security alerts, advisories and directives for customer-deployed resources (to include applications, operating systems, databases, and software). The customer control implementation statement should address the requirement that the customer receives system security alerts, advisories, and directives from customer-defined external organizations on an ongoing basis. |
| Part b | **Microsoft Azure (PaaS)**  Microsoft Azure implements this control for the operating systems supporting the PaaS environment.  Internal alerts are generated from tools within Microsoft Azure such as antivirus, Arbor Peakflow SP, and logging/monitoring tools.  Microsoft Azure also disseminates alerts received from vendor websites, 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 Resource Center (MSRC) which include specific information relevant to security updates being released. In general, only Critical and Important bulletins are reviewed by Microsoft Azure Security. The Microsoft Azure 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.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for managing security alerts, advisories and directives for customer-deployed resources. The customer control implementation statement should address how the customer generates internal security alerts, advisories, and directives as deemed necessary. |
| Part c | **Microsoft Azure (PaaS)**  Microsoft Azure implements this control for the operating systems supporting the PaaS environment.  Security alerts, advisories, and directives are disseminated to appropriate Microsoft Azure personnel as identified in the roles and responsibilities section of the Software Change and Release Management SOP and Hardware Change and Release Management SOP, and other properties throughout the organization.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for managing security alerts, advisories and directives for customer-deployed resources. The customer control implementation statement should address how the customer disseminates security alerts, advisories, and directives to: customer-defined personnel/roles, organizational elements, and/or external organizations. |
| Part d | **Microsoft Azure (PaaS)**  Microsoft Azure implements this control for the operating systems supporting the PaaS environment.  On receipt of the list of updates from MSRC, the RDOS team conducts an analysis to determine the applicability of the patches for Fabric Managed OS with the intent that all patches excepting those that are specifically not applicable to the code running on their servers will be applied.  If the RDOS team decides not to apply a patch as it is not applicable for the Base Images used in the Microsoft Azure environment, then the RDOS team will create a patch exception request ticket in TFS. This request is then reviewed and approved by the Microsoft Azure Security team. A justification for not selecting the patches including the details of the non-applicable patches is documented in TFS. The patch is deemed applicable even if a process that could exploit the vulnerability is not running, but is installed in the environment.  The WALS team conducts an analysis on the list provided by the OSSC team to confirm its applicability in Microsoft Azure. On completion of the analysis, the Microsoft Azure operations teams prepare the “Final Monthly Patch List” specifying the vulnerabilities that will be patched. This list includes details such as the Bulletin ID and Parent KB. 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 vulnerabilities are risk reviewed by Microsoft Azure Security. Many Low Risk scan results are determined by Microsoft Azure Security to pose no risk to Microsoft Azure. In this case an exception is filed and the result is not remediated. If the result is determined to pose any risk to Microsoft Azure, 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 for stakeholder and Microsoft Azure Security review. Microsoft Azure Security also verifies degree of compliance using vulnerability scanners deployed in Microsoft Azure.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for managing security alerts, advisories and directives for customer-deployed resources. The customer control implementation statement should address how the customer implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance. |

#### SI-5 (1) Control Enhancement (H)

The organization employs automated mechanisms to make security alert and advisory information available throughout the organization.

| SI-5 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-5 (1) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for managing security alerts, advisories and directives for customer-deployed resources. The customer control implementation statement should address the automated mechanisms used to make security alert and advisory information available throughout the organization. |

### 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: *<Customer-defined>*; Microsoft Azure | |
| Parameter SI-6(a): *<Customer-defined security functions>* | |
| Parameter SI-6(b): *<FedRAMP Assignment: to include upon system startup and/or restart at least monthly>* | |
| Parameter SI-6(c): *<FedRAMP Assignment: to include system administrators and security personnel>* | |
| Parameter SI-6(d)-1: *<Selection (one or more): shuts the information system down; restarts the information system>* | |
| Parameter SI-6(d)-2: *<FedRAMP Assignment: to include notification of system administrators and security 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-6 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure is responsible for verifying the security controls of the operating systems supporting the PaaS environment.  Microsoft Azure systems in Microsoft Azure Virtual Environment  Microsoft Azure performs periodic audit of the security functions to confirm their operating effectiveness via ASM. ASM monitors for the following areas:   * Unexpected change in firewall settings on root partition or platform service node * Unexpected processes executing on root partition or platform service node * Unexpected drivers installed on root partition or platform service node * Unexpected inbound or outbound traffic * Unexpected user account creation or logon sessions * Unexpected group creation * Although ASM monitors for the above security parameters alerts are generated only for the following * Unexpected drivers installed on root partition or platform service node * Unexpected user account creation * Unexpected group creation   ASM and MAs run continuously and monitor in real-time. ASM data is first written to local tables and then scheduled tasks specified in the monitoring configuration control the aggregation and uploading of the local data to the MDS store. Each detector uses a pair of tables: an anomaly table and a baseline table. The anomaly table contains records reflecting the results of any local analysis being done.  Microsoft Azure also uses applications called runners to monitor the collected data and Azure components, and report on the overall health of the system. If the overall health of system is deemed inappropriate for the environment by the system, the Fabric Controller (FC) is notified and the unhealthy system is shut down and a new healthy system is brought up somewhere else in the fabric.  Microsoft Azure Servers  Microsoft Azure verifies the correct operation of security functions of the physical servers upon system startup and/or restart and quarterly during vulnerability and configuration scanning as defined in RA-5 and CM-6(3).  Microsoft Azure SQL DB  WinFabric Platform  Microsoft Azure SQL DB leverages the components of the WinFabric platform which provides several critical capabilities for operating the Microsoft Azure SQL DB service.  The WinFabric platform provides a real-time monitoring framework that allows programmatic access to system health and performance data from outside the cluster. The monitoring framework provides a standard authentication, authorization (2FA) and query routing model and allows the application to expose application-specific monitoring data by providing custom monitoring listeners that plug-in to the framework. For example, in Microsoft Azure SQL DB, the GPM component includes a monitoring listener that exposes information about partition and replica status and health. This component monitors the partitions replications to detect which are up and down. These are monitored at startup and shutdown.  Runtime health reporting is integrated into an automated repair framework which enables regular hardware and software errors detected by application and system code to be automatically corrected without operator intervention to make the system self-healing.  The WinFabric platform watchdogs run continuously and monitor in real-time.  **Customer Responsibility (PaaS)**  The customer is responsible for security function verification for customer-deployed resources (to include applications, databases, and software). The customer control implementation statement should address the mechanisms used to verify the correct operation of customer-defined security functions.  **Customer Responsibility (IaaS)**  The customer is responsible for security function verification for customer-deployed resources (to include applications, operating systems, databases, and software). The customer control implementation statement should address the mechanisms used to verify the correct operation of customer-defined security functions. |
| Part b | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure is responsible for verifying the security controls of the operating systems supporting the PaaS environment.  See part a of this control for security functionality verification frequency, as it varies by verification method.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for security function verification for customer-deployed resources. The customer control implementation statement should address the performance of security function verification at customer-defined system transitional states (e.g., startup, restart, shutdown, abort) and/or upon command by a user with appropriate privilege, including the customer-defined frequency with which verification is performed. |
| Part c | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure monitoring tools generate alerts to service engineer personnel in the case of security functionality failure.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for security function verification for customer-deployed resources. The customer control implementation statement should address the notification of customer-defined personnel/roles of failed security verification tests. |
| Part d | **Microsoft Azure (IaaS/PaaS)**  Microsoft Azure monitoring tools generate alerts to service engineer personnel in the case of security functionality failure. Depending on the type of issue, TFS or Incident Management (ICM) tickets are opened to track resolution of the incident following the Incident Response process.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for security function verification for customer-deployed resources. The customer control implementation statement should address whether shutdown, restart, and/or an alternative customer-defined action is taken when anomalies are discovered. |

### 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-7 | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>*; Microsoft Azure | |
| Parameter SI-7: *<Customer-defined software, and 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-7 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (PaaS)**  Microsoft Azure is responsible for integrity verification of the operating systems supporting the PaaS environment.  Microsoft Azure software updates are thoroughly reviewed for any unauthorized changes before entering the production environments as part of the SDL and Change and Release Management processes. Any code changes have to be reviewed and approved before they are deployed to the environment. Additionally, builds are digitally signed before they are deployed. If the integrity verification fails at deployment, the deployment operation fails and the process needs to be started over.  Microsoft Azure components have a set of runners, which leverage information captured by MDS to run automated tests for checking the health of the components. Runners are configured to automatically generate alerts using Windows AIMS if any discrepancies are identified.  Microsoft Azure also utilizes Nessus for integrity scanning along with ASM to help reduce the risk of software components and devices potentially being tampered within the Microsoft Azure operating environment. ASM works as an extension of Microsoft Azure monitoring system which has components that observe, analyze and report on security events in Microsoft Azure operating environment. It complements the Azure security model by examining constraints that should remain valid at all times which encompasses configuration settings.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (PaaS)**  The customer is responsible for protecting software and information integrity for customer-deployed resources (to include applications, databases, and software). The customer control implementation statement should address the integrity verification tools used to detect unauthorized changes to customer-defined software and information.  **Customer Responsibility (IaaS)**  The customer is responsible for protecting software and information integrity for customer-deployed resources (to include applications, operating systems, databases, and software). The customer control implementation statement should address the integrity verification tools used to detect unauthorized changes to customer-defined software and information. |

#### 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-7 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>*; Microsoft Azure | |
| Parameter SI-7(1)-1: *<Customer-defined software, and information>* | |
| Parameter SI-7(1)-2: *<FedRAMP Assignment: to include security-relevant events>* | |
| Parameter SI-7(1)-3: *<FedRAMP Assignment: 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-7 (1) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (PaaS)**  Microsoft Azure is responsible for integrity verification of the operating systems supporting the PaaS environment.  Microsoft Azure software updates are reviewed for any unauthorized changes before entering the production environments as part of the SDL and Change and Release Management processes.  Microsoft Azure components have a set of runners, which leverage information captured by MDS to run automated tests for checking the health of the components. Runners are configured to automatically generate alerts using Windows AIMS if any discrepancies are identified.  Microsoft Azure also utilizes Nessus for integrity scanning along with ASM to help reduce the risk of software components and devices potentially being tampered within the Microsoft Azure operating environment. ASM works as an extension of the Microsoft Azure monitoring system which has components that observe, analyze and report on security events, including malware alerts, in the Microsoft Azure operating environment.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for protecting software and information integrity for customer-deployed resources. The customer control implementation statement should address the performance of integrity checks of customer-defined software and information at customer-defined system transitional states (e.g., startup, restart, shutdown, abort) or in response to security-related events, and the customer-defined frequency with which integrity checks are performed. |

#### SI-7 (2) Control Enhancement (H)

The organization employs automated tools that provide notification to [Assignment: organization- defined personnel or roles]] upon discovering discrepancies during integrity verification.

| SI-7 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter SI-7 (2): <Customer-defined personnel or roles> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-7 (2) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for protecting software and information integrity for customer-deployed resources. The customer control implementation statement should address how the customer employs automated tools that provide notification to customer-defined personnel/roles upon discovering discrepancies during integrity verification. |

#### SI-7 (5) Control Enhancement (H)

The information system automatically [Selection (one or more): shuts the information system down; restarts the information system; implements [Assignment: organization-defined security safeguard]] when integrity violations are discovered.

| SI-7 (5) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Parameter SI-7 (5): *<Customer-defined Selection (one or more): shuts the information system down; restarts the information system; implements customer-defined security safeguard>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-7 (5) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for automatically responding to integrity violations within customer-deployed resources. The customer control implementation statement should address the mechanisms used to automatically shut down or restart customer-deployed resources, and/or implement customer-defined security safeguards, when integrity violations are discovered. |

#### 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-7 (7) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>*; Microsoft Azure | |
| Parameter SI-7 (7): *<Customer-defined security-relevant changes to the information 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-7 (7) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (PaaS)**  Microsoft Azure implements this control for the operating systems supporting the PaaS environment.  As part of the software and information integrity checks, events are logged and tickets are opened in TFS and ICM for security-related events such as unauthorized changes to operating system files, installation of software, and privilege escalation. These incidents are then handled via the Incident Response process.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for protecting software and information integrity for customer-deployed resources. The customer control implementation statement should address how the customer incorporates the detection of unauthorized customer-defined security-relevant changes to customer-deployed resources into the incident response capability. |

#### SI-7 (14) Control Enhancement (H)

The organization:

1. Prohibits the use of binary or machine-executable code from sources with limited or no warranty and without the provision of source code; and
2. Provides exceptions to the source code requirement only for compelling mission/operational requirements and with the approval of the authorizing official.

| SI-7 (14) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-7 (14) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (IaaS/PaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (IaaS/PaaS)**  The customer is responsible for protecting software and information integrity for customer-deployed resources. The customer control implementation statement should address the mechanisms used to prohibit binary/machine-executable code from sources with limited or no warranty and without source code. These restrictions only occur for compelling mission/operational requirements and with the approval of the authorizing official. |

### 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: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-8 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (PaaS)**  Microsoft Azure does not host mail servers for its customers, thus spam protection is not applicable.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer responsibility (PaaS)**  Microsoft Azure does not host mail servers for its customers, thus spam protection is not applicable.  **Customer Responsibility (IaaS)**  The customer is responsible for employing spam protection. The customer control implementation statement should address the mechanisms in place at entry and exit points which detect and take action on unsolicited messages. Note: this control is only applicable to the customer if customer-deployed resources include an email server. |
| Part b | **Microsoft Azure (PaaS)**  Microsoft Azure does not host mail servers for its customers, thus spam protection is not applicable.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer responsibility (PaaS)**  Microsoft Azure does not host mail servers for its customers, thus spam protection is not applicable.  **Customer Responsibility (IaaS)**  The customer is responsible for employing spam protection. The customer control implementation statement should address how the mechanisms in SI-08.a are updated in accordance with organization policy and procedures. Note: this control is only applicable to the customer if customer-deployed resources include an email server. |

#### SI-8 (1) Control Enhancement (M) (H)

The organization centrally manages spam protection mechanisms.

| SI-8 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-8 (1) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (PaaS)**  Microsoft Azure does not host mail servers for its customers, thus spam protection is not applicable.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer responsibility (PaaS)**  Microsoft Azure does not host mail servers for its customers, thus spam protection is not applicable.  **Customer Responsibility (IaaS)**  The customer is responsible for employing spam protection. The customer control implementation statement should address how the mechanisms in SI-08.a are centrally managed. Note: this control is only applicable to the customer if customer-deployed resources include an email server. |

#### SI-8 (2) Control Enhancement (M) (H)

The organization automatically updates spam protection mechanisms.

| SI-8 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: *<Customer-defined>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-8 (2) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (PaaS)**  Microsoft Azure does not host mail servers for its customers, thus spam protection is not applicable.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer responsibility (PaaS)**  Microsoft Azure does not host mail servers for its customers, thus spam protection is not applicable.  **Customer Responsibility (IaaS)**  The customer is responsible for employing spam protection. The customer control implementation statement should address how the mechanisms in SI-08.a are automatically updated. Note: this control is only applicable to the customer if customer-deployed resources include an email server. |

### 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: *<Customer-defined>*; Microsoft Azure | |
| Parameter SI-10: *<Customer-defined 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-10 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (PaaS)**  Microsoft Azure implements this control for the operating systems supporting the PaaS environment.  Microsoft Azure follows system development methodology and security guidelines outlined in the Microsoft Azure Security Policy. In addition, Microsoft Azure service offerings also adhere to the Microsoft Security Development Lifecycle (SDL) requirements described in the common Online Services Secure Coding procedure. The SDL process addresses requirements around input data validation within applications.  Microsoft Azure has implemented information validation through checking of data inputs as part of the SDL process. Thorough code reviews and testing are completed during the Verification Phase of the SDL prior to 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.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (PaaS)**  The customer is responsible for information input validation for customer-deployed resources (to include applications, databases, and software). The customer control implementation statement should address the mechanisms used to check the validity of customer-defined information inputs.  **Customer Responsibility (IaaS)**  The customer is responsible for information input validation for customer-deployed resources (to include applications, operating systems, databases, and software). The customer control implementation statement should address the mechanisms used to check the validity of customer-defined information inputs. |

### 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: *<Customer-defined>*; Microsoft Azure | |
| Parameter SI-11(b): *<Customer-defined personnel or roles>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-11 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure (PaaS)**  Microsoft Azure implements this control for the operating systems supporting the PaaS environment.  Microsoft Azure 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 Microsoft Azure users.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (PaaS)**  The customer is responsible for generating error messages for customer-deployed resources (to include applications, databases, and software). The customer control implementation statement should address how error messages are used to provide information necessary for corrective actions without revealing information that could be exploited by adversaries.  **Customer Responsibility (IaaS)**  The customer is responsible for generating error messages for customer-deployed resources (to include applications, operating systems, databases, and software). The customer control implementation statement should address how error messages are used to provide information necessary for corrective actions without revealing information that could be exploited by adversaries. |
| Part b | **Microsoft Azure (PaaS)**  Microsoft Azure 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 Microsoft Azure users.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (PaaS)**  The customer is responsible for revealing the error messages defined in SI-11.a. The customer control implementation statement should address how they are revealed only to customer-defined personnel/roles.  **Customer Responsibility (IaaS)**  The customer is responsible for revealing the error messages defined in SI-11.a. The customer control implementation statement should address how they are revealed only to customer-defined personnel/roles. |

### 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-defined>;* Microsoft 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-12 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (PaaS)**  Microsoft Azure implements this control for the operating systems supporting the PaaS environment.  Microsoft Azure-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 Microsoft Azure asset inventory. Refer to Corporate Records Management’s Microsoft Corporate Document Retention Schedule (available for onsite review), which describes which Microsoft documents must be kept and for how long.  **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (PaaS)**  The customer is responsible for handling and retaining information within customer-deployed resources (to include applications, databases, and software) and information output from those resources. The customer control implementation statement should address how information handling and retention is performed in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.  **Customer Responsibility (IaaS)**  The customer is responsible for handling and retaining information within customer-deployed resources (to include applications, operating systems, databases, and software) and information output from those resources. The customer control implementation statement should address how information handling and retention is performed in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements. |

### 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: *<Customer-defined>*; Microsoft Azure | |
| Parameter SI-16-1: *<Customer-defined fail-safe 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 FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-16 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure (PaaS)**  Microsoft Azure is responsible for implementing the protection of memory executing unauthorized code for operating systems supporting the PaaS environment.  Microsoft Azure uses Windows and Ubuntu Linux servers for its services. Both of these operating systems have protections in place for preventing code execution in restricted memory locations: No Execute (NX), Address Space Layout Randomization (ASLR), and Data Execution Prevention (DEP).  Additionally, the Microsoft SDL requires secure coding practices including explicit consideration for safe memory handling requirements.  See the following TechNet articles for more information about the aforementioned 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   **Microsoft Azure (IaaS)**  The customer is responsible for implementing this control.  **Customer Responsibility (PaaS)**  The customer is responsible for protecting customer-deployed resources (to include applications, databases, and software) from unauthorized code execution. The customer control implementation statement should address the customer-defined security safeguards to protect the memory of customer-deployed resources from unauthorized code execution.  **Customer Responsibility (IaaS)**  The customer is responsible for protecting customer-deployed resources (to include applications, operating systems, databases, and software) from unauthorized code execution. The customer control implementation statement should address the customer-defined security safeguards to protect the memory of customer-deployed resources from unauthorized code execution. |

# Acronyms

The master list of FedRAMP acronym and glossary definitions for all FedRAMP templates is available on the FedRAMP website [Documents](https://www.fedramp.gov/resources/documents-2016/) page under Program Overview Documents.

Please send suggestions about corrections, additions, or deletions to info@fedramp.gov.

SYSTEMS SECURITY PLAN ATTACHMENTS

Instruction: Attach any documents that are referred to in the Information System Name (Information System Abbreviation) System Security Plan. Documents and attachments should, provide the title, version and exact file name, including the file extension. All attachments and associated documents must be delivered separately. No embedded documents will be accepted.

Delete this and all other instructions from your final version of this document.

# 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 Information System Abbreviation 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 ‑. Attachment File Naming Convention

|  |  |  |
| --- | --- | --- |
| Attachment | File Name | File Extension |
| Information Security Policies and Procedures | Information System Abbreviation A1 ISPP xx v1.0 | . enter extension |
| User Guide | Information System Abbreviation A2 UG v1.0 | . enter extension |
| E-Authentication Worksheet | Included in Section 15 |  |
| PTA | Included in Section 15 |  |
| PIA (if needed) | Information System Abbreviation A4 PIA v1.0 | . enter extension |
| Rules of Behavior | Information System Abbreviation A5 ROB v1.0 | . enter extension |
| Information System Contingency Plan | Information System Abbreviation A6 ISCP v1.0 | . enter extension |
| Configuration Management Plan | Information System Abbreviation A7 CMP v1.0 | . enter extension |
| Incident Response Plan | Information System Abbreviation A8 IRP v1.0 | . enter extension |
| CIS Summary Report | Information System Abbreviation A9 CIS Report v1.0 | . enter extension |
| CIS Worksheet | Information System Abbreviation A9 CIS WSv1.0 | . enter extension |
| FIPS 199 | Included in Section 15 |  |
| Inventory | Information System Abbreviation A13 INV v1.0 | . enter extension |

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.

ATTACHMENT 2 - User Guide

All Authorization Packages must include a User Guide attachment, which will be reviewed for quality.

ATTACHMENT 3 – e-Authentication Worksheet

This Attachment Section has been revised to include the e-Authentication template. Therefore, a separate attachment is not needed. Delete this note and all other instructions from your final version of this document.

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.

### 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](http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf)

### Information System Name/Title

This E-Authentication Plan provides an overview of the security requirements for the Information System Name (Information System Abbreviation) in accordance with OMB Memo M-04-04.

Table 15‑2 Information System Name and Title

| Unique Identifier | Information System Name | Information System Abbreviation |
| --- | --- | --- |
| Enter FedRAMP Application Number. | Information System Name | Information System Abbreviation |

### 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](http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf)

### Review Maximum Potential Impact Levels

CSP Name has assessed the potential risk from E-Authentication errors, or E-Authentication misuse, related to a user’s asserted identity. CSP Name 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

Instruction: Select the lowest level that will cover all potential impact identified from Table 15‑3 Potential Impacts for Assurance Levels.

Delete this instruction from your final version of this document.

The CSP Name 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: multi-factor remote authentication | Moderate |  |
| Level 4: multi-factor remote authentication; hard crypto tokens | High |  |

ATTACHMENT 4 – PTA / PIA

This Attachment Section has been revised to include the PTA Template. Therefore, a separate PTA attachment is not needed. If any of the answers to Question 1-4 are “Yes” then complete a Privacy Impact Assessment Template and include it as an Attachment.

Delete this note and all other instructions from your final version of this document.

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.

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 CSP Name.

Table ‑ - Information System Name; Privacy POC

| Name | Click here to enter text. |
| --- | --- |
| Title | Click here to enter text. |
| CSP / Organization | Click here to enter text. |
| Address | Click here to enter text. |
| Phone Number | Click here to enter text. |
| Email Address | Click here to enter text. |

#### 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 Information System Name Laws and Regulations include additional laws and regulations that are specific to <Information System Name>. 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 ‑ <Information System Name> Laws and Regulations

| Identification Number | Title | Date | Link |
| --- | --- | --- | --- |
| Click here to enter text. | Click here to enter text. | Click here to enter text. | Click here to enter text. |
| Click here to enter text. | Click here to enter text. | Click here to enter text. | Click here to enter text. |

#### 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 Information System Name Standards and Guidance includes any additional standards and guidance that are specific to <Information System Name>. These will include standards and guidance from Federal Information Processing Standard (FIPS) and National Institute of Standards and Technology (NIST) Special Publications (SP).

Table ‑ <Information System Name> Standards and Guidance

| Identification Number | Title | Date | Link |
| --- | --- | --- | --- |
| Click here to enter text. | Click here to enter text. | Click here to enter text. | Click here to enter text. |
| Click here to enter text. | Click here to enter text. | Click here to enter text. | Click here to enter text. |

#### 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

CSP Name performs a Privacy Threshold Analysis annually to determine if PII is collected by any of the <Information System Name> (Information System Abbreviation) components. If PII is discovered, a Privacy Impact Assessment is performed. The Privacy Impact Assessment template used by CSP Name can be found in Section 3. This section constitutes the Privacy Threshold Analysis and findings.

#### Qualifying Questions

|  |  |
| --- | --- |
| Select One | Does the ISA collect, maintain, or share PII in any identifiable form? |
| Select One | Does the ISA collect, maintain, or share PII information from or about the public? |
| Select One | Has a Privacy Impact Assessment ever been performed for the ISA? |
| Select One | 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. |

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.

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.

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.

ATTACHMENT 8 - Incident Response Plan

All Authorization Packages must include an Incident Response Plan attachment, which will be reviewed for quality.

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.

Templates for both can be found on the following FedRAMP website page: [Templates](https://www.fedramp.gov/resources/templates-2016/).

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

This Attachment Section has been revised to include the FIPS 199 Template. Therefore, a separate PTA attachment is not needed. Delete this note and all other instructions from your final version of this document.

All Authorization Packages must include a Federal Information Processing Standard (FIPS) 199 Section, which will be reviewed for quality.

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 <Information System Name> system has been determined to have a security categorization of Choose level.

Instruction: Insert a brief high-level description of the system, the system environment and the purpose of the system. The description should be consistent with the description found in the System Security Plan (SSP).   
Delete this instruction from your final version of this document.

### Methodology

Instruction: The CSP should review the NIST Special Publication 800-60 Volume 2 Revision 1 Appendix C Management and Support Information and Information System Impact Levels and Appendix D Impact Determination for Mission-Based Information and Information Systems to assess the recommended impact level for each of the information types. For more information, the CSP should also consult Appendix D.2. After reviewing the NIST guidance on Information Types, the CSP should fill out Table 15‑8 CSP Applicable Information Types with Security Impact Levels Using NIST SP 800-60 V2 R1.   
Delete this instruction from your final version of this document.

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.

Instruction: In the first three columns, put the NIST SP-60 V2 R1 recommended impact level. In the next three columns, put in the CSP determined recommended impact level. If the CSP determined recommended impact level does not match the level recommended by NIST, put in an explanation in the last column as to why this decision was made.   
Delete this instruction from your final version of this document.

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 ‑ 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 |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. |
| Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. |
| Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. |
| Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. |
| Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. |
| Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. |
| Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. |
| Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. |
| Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. |
| Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. |
| Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. |
| Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. |
| Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. | Enter text. |

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.

ATTACHMENT 11 - Separation of Duties Matrix is referenced in the following controls.

AC-5 Separation of Duties (M) (H) Additional FedRAMP Requirements and Guidance

ATTACHMENT 12 – FedRAMP Laws and Regulations

The Table 15‑9 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.

Table ‑ 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](https://www.fedramp.gov/resources/templates-2016/).

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.

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](https://www.fedramp.gov/resources/templates-2016/).

Note: A complete and detailed list of the system hardware and software inventory is required per NIST SP 800-53, Rev 4 CM-8.