Microsoft Azure Blueprint  
Control Implementation Guidance

|  |
| --- |
|  |

Red Hat OpenShift v3 on Microsoft Azure for Government

Version 1.0

10/20/2016

This document is provided for informational purposes only. You are solely responsible for developing, implementing, and managing your applications and/or subscriptions running on Microsoft Azure and Azure Government in compliance with applicable laws, regulations, and contractual obligations.  This document is provided "AS-IS" and without any warranty of any kind, whether in express, implied or statutory, and Microsoft expressly disclaims all warranties of merchantability, fitness for a particular purpose, or non-infringement.

1. Customer Responsibility

This section describes control implementation for which the customer will be responsible. For each control, the control requirements are stated first, followed by boxes which must be filled out with a description of how the customer application meets those requirements. FedRAMP has provided the following guidance:

***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 provided in some way by the service provider.*

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

*For SaaS and PaaS systems that are inheriting controls from an IaaS (or anything lower in the stack), 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.*

*In section 13, the NIST term "organization defined" must be interpreted as being the CSP's responsibility unless otherwise indicated. In some cases the JAB has chosen to define or provide parameters, in others they have left the decision up to the CSP.*

***Customer Responsibility Attachment***

*Azure’s Customer Responsibility Matrix (CRM) attachment denotes the list of controls alongside the control implementation narrative for IaaS and 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. Multifactor Authentication Implementation may be a potential example where it is not feasible for an Agency or 3rd Party provider to transfer such responsibility onto an external customer.*

| **Control Origination** | **Definition** | **Example** |
| --- | --- | --- |
| Service Provider Corporate | A control that originates from the CSP 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 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. | 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 and partially by the customer. | Security awareness training must be conducted by both the CSP and the customer. |
| Inherited from pre-existing Provisional Authorization | A control that is inherited from another CSP system that has already received a Provisional Authorization. | A PaaS or SaaS provider inherits PE controls from an IaaS provider. |

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. Should include a description of why the requirement does not apply.

**Control Origination**: See the FedRAMP-provided table above. In addition, note the following:

* The CSP in this context is you, the Microsoft customer. Controls for which Microsoft is responsible are marked as “Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure”.
* The customer in this context is any entity outside your organization using your services.
* 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 of the 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. Text in the following format should be replaced with customer-created content:

<*The customer is responsible for meeting the requirements of this control.*>

This italicized text will include a summary of the relevant control requirements, guidance on writing a successful control response, and links to Azure documentation or other security-related documentation where applicable.

Some controls are implemented in whole or in part by Microsoft Azure on behalf of IaaS or PaaS customers. In this case, the text will include a reference to Part 14 (IaaS) or Part 15 (PaaS) for further details.

Microsoft has pre-selected checkboxes, which you should review and update as applicable for your system. In cases where the control is fully inherited from IaaS or PaaS, the checkboxes should remain as-is.

* 1. Access Control (AC)
     1. Access Control Policy and Procedures (AC-1)

The organization:

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

| AC-1 | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter AC-1(a): <*Customer-defined personnel or roles*> | |
| Parameter AC-1(b)1: <*FedRAMP requirement: at least every 3 years*> | |
| Parameter AC-1(b)2: <*FedRAMP requirement: 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) | |

| AC-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for developing, documenting, and disseminating Access Control policy and procedures. A successful control response will need to address the content of the policy (which must include purpose, scope, roles, responsibilities, management commitment, coordination, and compliance) and procedures (which must facilitate the implementation of the policies and associated controls).*>  *<Adding, or binding, a role to users or groups gives the user or group the relevant access granted by the role. You can add and remove roles to and from users and groups using OpenShift commands. Documentation for the management of Role Bindings can be found at* [*https://docs.openshift.com/container-platform/latest/admin\_guide/manage\_authorization\_policy.html#managing-role-bindings*](https://docs.openshift.com/container-platform/latest/admin_guide/manage_authorization_policy.html#managing-role-bindings)*>* |
| Part b | **Customer Responsibility**  <*The customer will be responsible for reviewing and updating the Access Control policy every 3 years, and procedures annually. A successful control response will need to address the review and update process, including the role(s) responsible for initiating the review process, updating the policy and procedures, and providing approval of the updates.*> |

* + 1. Account Management (AC-2)

The organization:

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

| AC-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 requirement: at least annually*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| AC-2 What is the solution and how is it implemented? | | |
| --- | --- | --- |
| Part a | | **Customer Responsibility**  <*The customer will be responsible for identifying and selecting the types of accounts required to support the customer application. Examples of account types include individual, shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and service. A successful control response will need to address the specific requirements fulfilled by each account type in use.*  *Microsoft’s Trust Center has resources related to identity and access management. For example:*   * [*https://www.microsoft.com/en-us/TrustCenter/Security/Identity*](http://www.commoncriteriaportal.org/products.html) *discusses the use of Azure Active Directory (AAD) and Azure Multi-Factor Authentication to manage customer access* * [*https://azure.microsoft.com/en-us/documentation/articles/multi-factor-authentication-security-best-practices/*](http://technet.microsoft.com/en-us/library/cc771361(v=WS.10).aspx) *addresses the use of Multi-Factor Authentication in more detail* * [*https://azure.microsoft.com/en-us/documentation/articles/active-directory-hybrid-identity-design-considerations-overview/*](http://usgcb.nist.gov/usgcb_faq.html) *addresses the integration of cloud-based identity management with existing on-premises identity management solutions*> |
| Part b | | **Customer Responsibility**  <*The customer will be responsible for assigning account managers, who will have responsibilities related to the creation, management, and removal of accounts. A successful control response will need to discuss how account managers are identified within the organization.*> |
| Part c | | **Customer Responsibility**  <*The customer will be responsible for setting conditions for group and role membership. A successful control response will need to outline these conditions and how they are enforced.*> |
| Part d | | **Customer Responsibility**  <*The customer will be responsible for specifying authorized users, group and role membership, and privileges for each account. A successful control response will need to address the process by which authorized users are specified and privilege levels are determined.*> |
| Part e | | **Customer Responsibility**  <*The customer will be responsible for requiring approval by designated personnel or roles prior to creating information system accounts. A successful control response will need to outline the personnel or roles responsible for approving information system accounts and the process by which those personnel or roles are notified and approval is granted.*> |
| Part f | | **Customer Responsibility**  <*The customer will be responsible for defining and enforcing procedures or conditions for the creation, management, and removal of information system accounts. A successful control response will outline the conditions for each action and the tools or procedures used to enforce those conditions.*> |
| Part g | **Customer Responsibility**  <*The customer will be responsible for monitoring the use of information system accounts. This may include reviewing records of account management activities in the Microsoft Azure Management Portal. A successful control response will relate the monitoring activities required for this control to the auditing activities in the AU control family.*> | |
| Part h | | **Customer Responsibility**  <*The customer will be responsible for notifying account managers when accounts are no longer required, when users are terminated or transferred, or when system usage or need-to-know changes. A successful control response will need to address the methods by which these triggering events are identified and the managers are notified.*> |
| Part i | | **Customer Responsibility**  <*The customer will be responsible for authorizing access to the customer application. A successful control response will need to address ensuring that all accounts are granted access based on a valid authorization for a specific intended usage.*> |
| Part j | | **Customer Responsibility**  <*The customer will be responsible for reviewing accounts for compliance with account management requirements at the specified frequency. A successful control response will need to address the process used to review accounts, the means by which compliance is verified, and the process for remediation of any accounts found not to be in compliance.*> |
| Part k | | **Customer Responsibility**  <*The customer will be responsible for reissuing shared/group account credentials when individuals are removed from the group. A successful control response will need to discuss how a triggering event is notified, what the process and timeframe for reissuing credentials is, and how the process is enforced.*> |

* + - 1. Control Enhancement AC-2 (1)

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

| AC-2 (1) | Control Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| AC-2 (1) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for employing automated mechanisms to support account management activities. Microsoft’s AAD solution may be used for this purpose; see* [*https://www.microsoft.com/en-us/TrustCenter/Security/Identity*](https://www.microsoft.com/en-us/TrustCenter/Security/Identity) *for more information on the configuration and use of AAD. A successful control response will need to address all automated mechanisms used for account management.*>  <*For an understanding of what authentication configuration options are exposed in OpenShift v3, refer to* [*https://docs.openshift.com/container-platform/3.3/architecture/additional\_concepts/authentication.html*](https://docs.openshift.com/container-platform/3.3/architecture/additional_concepts/authentication.html) *>* |

* + - 1. Control Enhancement AC-2 (2)

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

| AC-2 (2) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter AC-2(2)-1: <*Customer selection (removes or disables)*> | |
| Parameter AC-2(2)-2: <*FedRAMP requirement: no more than 30 days for temporary and emergency account types*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| AC-2 (2) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for automatically removing or disabling emergency and temporary accounts within the required timeframe. Microsoft’s AAD solution may be used in support of this purpose; see* [*https://www.microsoft.com/en-us/TrustCenter/Security/Identity*](http://technet.microsoft.com/en-us/library/bb457155.aspx) *for more information on the configuration and use of AAD. A successful control response will need to address all of the procedures and mechanisms involved in disabling these accounts.*>  *<OpenShift does not have the capability to automatically disable accounts after a configured period of time. To meet this requirement, an authentication provider (such as Active Directory) must be used. Integration between OpenShift and Active Directory can be accomplished through the use of Kerberos cross-realm trusts. Refer to the “LDAP Authentication” section of the OpenShift Administrators guide:* [*https://docs.openshift.com/container-platform/3.3/admin\_solutions/authentication.html#ldap-auth*](https://docs.openshift.com/container-platform/3.3/admin_solutions/authentication.html#ldap-auth)*>.* |

* + - 1. Control Enhancement AC-2 (3)

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

**AC-2 (3) Parameter 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 Authorizing Official.

|  |  |
| --- | --- |
| AC-2 (3) | Control Enhancement Summary Information |
| Responsible Role: <*Customer defined*> | |
| Parameter AC-2(3): <*FedRAMP requirement: 90 days for user accounts*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Configured by customer  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| AC-2 (3) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for automatically disabling user accounts after the specified period of inactivity. Microsoft’s AAD solution may be used for this purpose; see* [*https://www.microsoft.com/en-us/TrustCenter/Security/Identity*](https://azure.microsoft.com/en-us/documentation/articles/multi-factor-authentication-security-best-practices/) *for more information on the configuration and use of AAD. A successful control response will need to address all automated mechanisms involved in disabling inactive accounts.*>  *<OpenShift does not have the capability to automatically disable accounts after a configured period of time. To meet this requirement, an authentication provider (such as Active Directory) must be used. Integration between OpenShift and Active Directory can be accomplished through the use of Kerberos cross-realm trusts. Refer to the “LDAP Authentication” section of the OpenShift Administrators guide:* [*https://docs.openshift.com/container-platform/3.3/admin\_solutions/authentication.html#ldap-auth*](https://docs.openshift.com/container-platform/3.3/admin_solutions/authentication.html#ldap-auth)*>* |

* + - 1. Control Enhancement AC-2 (4)

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

| AC-2 (4) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter AC-2(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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| AC-2 (4) What is the solutions and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for automatically auditing account management actions. Microsoft’s AAD solution may be used for this purpose; see* [*https://www.microsoft.com/en-us/TrustCenter/Security/Identity*](https://www.microsoft.com/en-us/TrustCenter/Security/Identity) *for more information on the configuration and use of AAD. A successful control response will need to address all automated mechanisms involved in monitoring account management, the personnel or roles that must be notified of account management actions, and the means by which notifications occur.*>  *<OpenShift will log events to standardized files, however automatic notification (outside of generating audit data) is not possible. As an OpenShift Container Platform cluster administrator, you can deploy the EFK stack to aggregate logs for a range of OpenShift Container Platform services and setup alerting. Application developers can view the logs of the projects for which they have view access. The EFK stack aggregates logs from hosts and applications, whether coming from multiple containers or even deleted pods. For documentation on how to setup Elasticsearch, Fluentd, and Kibana, refer to the “Aggregate Logging” section of the OpenShift Installation and Configuration Guide:* [*https://docs.openshift.com/container-platform/3.3/install\_config/aggregate\_logging.html*](https://docs.openshift.com/container-platform/3.3/install_config/aggregate_logging.html)*>* |

* + - 1. Control Enhancement AC-2 (5)

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

| AC-2 (5) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter AC-2(5): <*Customer defined requirements for log out*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| AC-2 (5) What is the solutions and how is it implemented? |
| --- |
| **Customer Responsibility**  The sessionMaxAgeSeconds variable in the master-config.yaml file |

* + - 1. Control Enhancement AC-2 (7)

The organization:

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

| AC-2 (7) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter AC-2(7)(c): <*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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| AC-2 (7) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for establishing and administering privileged accounts in accordance with a role-based access control (RBAC) scheme. Microsoft’s AAD solution may be used for this purpose; see* [*https://www.microsoft.com/en-us/TrustCenter/Security/Identity*](http://usgcb.nist.gov/usgcb_faq.html) *for more information on the configuration and use of AAD. A successful control response will need to address the types of users or roles that receive privileged access as well as the organization of the RBAC scheme.*>  *<Adding, or binding, a role to users or groups gives the user or group the relevant access granted by the role. You can add and remove roles to and from users and groups using OpenShift commands. Documentation for the management of Role Bindings can be found at* [*https://docs.openshift.com/container-platform/latest/admin\_guide/manage\_authorization\_policy.html#managing-role-bindings*](https://docs.openshift.com/container-platform/latest/admin_guide/manage_authorization_policy.html#managing-role-bindings)*>* |
| Part b | **Customer Responsibility**  <*The customer will be responsible for monitoring privileged role assignments. Microsoft’s AAD solution may be used for this purpose; see* [*https://www.microsoft.com/en-us/TrustCenter/Security/Identity*](https://www.microsoft.com/en-us/TrustCenter/Security/Identity) *for more information on the configuration and use of AAD. A successful control response will need to address the processes by which role assignments are reviewed for continued appropriateness.*> |
| Part c | **Customer Responsibility**  <*The customer will be responsible for defining and executing actions to take when privileged role assignments are no longer appropriate. Microsoft’s AAD solution may be used to support this purpose; see* [*https://www.microsoft.com/en-us/TrustCenter/Security/Identity*](https://www.microsoft.com/en-us/TrustCenter/Security/Identity) *for more information on the configuration and use of AAD. A successful control response will need to address the criteria for determining whether assignments are no longer appropriate, the actions to be taken, and the roles or personnel responsible for taking those actions.*> |

* + - 1. Control Enhancement AC-2 (9)

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

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

| AC-2 (9) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter AC-2(9): <*Customer defined requirements*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| AC-2 (9) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for defining and enforcing conditions for the use of shared or group accounts. A successful control response will need to address the specific need for the existing of a shared or group account versus multiple individual accounts, as well as the process for reviewing membership of shared or group accounts to verify that all individuals with access still require that access.*>  *<By default, OpenShift does not support group authenticators. OpenShift does provide a role-based access control (RBAC) mechanism and user identity metadata, including group membership. Identity and RBAC controls are enforced against all user (privileged and non-privileged) actions and resources. RBAC access controls can be applied to provide access to resources by individual users or groups of users. Grups are typically configured in accordance with Section 3.4, “Managing User and Group Labels” in OpenShift v3.3’s Cluster Administration Guide:* [*https://docs.openshift.com/container-platform/3.3/admin\_guide/manage\_users.html#managing-users-managing-user-and-group-labels*](https://docs.openshift.com/container-platform/3.3/admin_guide/manage_users.html#managing-users-managing-user-and-group-labels) *>* |

* + - 1. Control Enhancement AC-2 (10)

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 Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| AC-2 (10) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for terminating or changing credentials for shared or group accounts when membership to those groups changes. Microsoft’s AAD solution may be used for this purpose; see* [*https://www.microsoft.com/en-us/TrustCenter/Security/Identity*](https://www.microsoft.com/en-us/TrustCenter/Security/Identity) *for more information on the configuration and use of AAD. A successful control response will need to discuss how group membership change is detected and reported, the personnel or roles responsible for changing the affected credentials, and the process or mechanism used to perform the change.*> |

* + - 1. Control Enhancement AC-2 (12)

The organization:

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

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

| AC-2 (12) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter AC-2(12)(a): <*Customer defined atypical use*> | |
| Parameter AC-2(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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| AC-2 (12) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for monitoring information system accounts for atypical use. A successful control response will relate the monitoring activities required for this control to the auditing activities in the AU control family, and will discuss the criteria for atypical use.*>  *<OpenShift embeds the Elasticsearch, Fluentd, and Kibana (EFK) stack. This pre-integrated audit reduction capability aggregates logs from nodes and applications running inside your OpenShift Container Platform installation. Once deployed it uses Fluentd to aggregate event logs from all notes, projects, and pods into Elasticsearch (ES). It also provides a centralized Kibana web UI where users and administrators can create rich visualizations and dashboards with the aggregated data. Triggers may be setup to detect atypical use.*  *For aggregate log sizing information, refer to the “Aggregate Logging Sizing Guidelines” of the Installation and Configuration guide:* [*https://docs.openshift.com/container-platform/3.3/install\_config/aggregate\_logging\_sizing.html*](https://docs.openshift.com/container-platform/3.3/install_config/aggregate_logging_sizing.html)  *For instructions on how to configure aggregate logging, refer to the “Aggregating Container Logs” section of the Installation and Configuration guide: https://docs.openshift.com/container-platform/3.3/install\_config/aggregate\_logging.html>* |
| Part b | **Customer Responsibility**  <*The customer will be responsible for reporting atypical use of information system accounts. A successful control response will discuss the personnel or roles that must be notified and the process for notification.*> |

* + 1. Access Enforcement (AC-3)

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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| AC-3 What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*Documentation on OpenShift Authorization frameworks can be found online at* [*https://docs.openshift.com/container-platform/3.3/architecture/additional\_concepts/authorization.html*](https://docs.openshift.com/container-platform/3.3/architecture/additional_concepts/authorization.html)*. Each OpenShift deployment may chose different authorization processes/configurations..*> |

* + 1. Information Flow Enforcement (AC-4)

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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| AC-4 What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for controlling the flow of information within the customer application, and between the customer application and external systems. A successful control response will need to address the customer’s information flow control policies, as well as mechanisms in place to enforce those policies.*>  <*A review of OpenShift v3 networking can be found online:* [*https://docs.openshift.com/container-platform/3.3/architecture/additional\_concepts/networking.html*](https://docs.openshift.com/container-platform/3.3/architecture/additional_concepts/networking.html)> |

* + - 1. Control Enhancement AC-4 (21)

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 Enhancement 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 separation 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| AC-4 (21) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for separating information flows within the customer application. A successful control response will need to address the customer’s organizational requirements for the separation of information flows, and the mechanisms and techniques used to accomplish this separation.*>  *<A review of OpenShift networking can be found here:* [*https://docs.openshift.com/container-platform/3.3/architecture/additional\_concepts/networking.html*](https://docs.openshift.com/container-platform/3.3/architecture/additional_concepts/networking.html) *>* |

* + 1. Separation of Duties (AC-5)

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.

| 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| AC-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for defining separation of duties between individuals so as to reduce the risk of insider threat without collusion. A successful control response will need to consider the possible actions a malicious insider could take to undermine the security of the system, and delineate how duties are separated to prevent or reduce the likelihood of those actions.*> |
| Part b | **Customer Responsibility**  <*The customer will be responsible for documenting separation of duties. A successful control response will need to address the location of this documentation and the process for reviewing it if necessary.*> |
| Part c | **Customer Responsibility**  <*The customer will be responsible for defining access authorizations to support separation of duties, for example by using Role Based Access Control. A successful control response will need to address policy and technical enforcement of separation of duties.*> |

* + 1. Least Privilege (AC-6)

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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| AC-6 What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for following least-privilege principles when granting authorized accesses. A successful control response will need to address the use of business requirements to determine the level of access required to perform each job function, and how that is related to the role-based access control scheme used within the system.*> |

* + - 1. Control Enhancement AC-6 (1)

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

| AC-6 (1) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter AC-6(1): <*Customer defined security functions and security-relevant information*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| AC-6 (1) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for defining key security functions and security-relevant information, and for explicitly authorizing access to those functions and information. A successful control response will need to address the criteria used to determine which functions and information require explicit access authorization.*> |

* + - 1. Control Enhancement AC-6 (2)

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 nonsecurity 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 Enhancement Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter AC-6(2): <*FedRAMP requirement: all security functions*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| AC-6 (2) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for requiring users to use the lowest level of access required to perform any given function. A successful control response will need to discuss how the level of access in use is monitored and enforced.*> |

* + - 1. Control Enhancement AC-6 (5)

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

| AC-6 (5) | Control Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| AC-6 (5) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for defining specific personnel or roles who require privileged access, and restricting privileged access to those personnel or roles. A successful control response will need to address the job functions or responsibilities for which privileged access is required.*> |

* + - 1. Control Enhancement AC-6 (9)

The information system audits the execution of privileged functions.

| AC-6 (9) | Control Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| AC-6 (9) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for auditing the execution of privileged functions. A successful control response will need to relate this requirement to the general auditing requirements of the AU control family.*> |

* + - 1. Control Enhancement AC-6 (10)

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 Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| AC-6 (10) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for ensuring that non-privileged users cannot execute privileged functions. Microsoft’s AAD solution may be used to support this control by creating appropriate privileged and non-privileged roles; see* [*https://www.microsoft.com/en-us/TrustCenter/Security/Identity*](http://www.niap-ccevs.org/vpl) *for more information on the configuration and use of AAD. A successful control response will need to discuss the use of AAD and any other means of enforcement of privilege levels.*> |

* + 1. Unsuccessful Login Attempts (AC-7)

The organization:

1. Enforces a limit of [*FedRAMP Assignment: not more than three*] consecutive invalid logon attempts by a user during a [*FedRAMP Assignment: fifteen minutes*]; and
2. Automatically [*Selection: locks the account/node for an* [*FedRAMP Assignment: thirty minutes*]; *locks the account/node until released 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 Additional FedRAMP Requirements and Guidance:** Guidance: FedRAMP considers remote admin access by VPN to be remote access.

| AC-7 | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter AC-7(a)-1: <*FedRAMP requirement: not more than three*> | |
| Parameter AC-7(a)-2: <*FedRAMP requirement: fifteen minutes*> | |
| Parameter AC-7(b)-1: <*FedRAMP requirement: locks the account/node for thirty minutes*> | |
| Parameter AC-7(b)-2: <*Customer defined additional actions*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| AC-7 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for enforcing a limit on consecutive failed login attempts. Microsoft’s AAD solution may be used to support this purpose; see* [*https://www.microsoft.com/en-us/TrustCenter/Security/Identity*](https://www.microsoft.com/en-us/TrustCenter/Security/Identity) *for more information on the configuration and use of AAD.*> |
| Part b | **Customer Responsibility**  <*The customer will be responsible for taking the FedRAMP required actions, as well as any additional actions defined by the customer, upon account lockout. Microsoft’s AAD solution may be used to support this purpose; see* [*https://www.microsoft.com/en-us/TrustCenter/Security/Identity*](https://www.microsoft.com/en-us/TrustCenter/Security/Identity) *for more information on the configuration and use of AAD*> |

* + 1. System Use Notification (AC-8)

The information system:

1. Displays to users [*Assignment: organization-defined system use notification message or banner (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
3. For publicly accessible systems:
   1. Displays system use information [*Assignment: organization-defined conditions (See Additional Requirements and Guidance)*], before granting further access;
   2. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
   3. 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.

**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.

**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.

| AC-8 | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter AC-8(a): <*Customer defined system use notification 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| AC-8 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for displaying a system use notification banner to users. A successful control response will need to address the conditions under which the banner will be displayed (if a non-government user accesses the system, the system use notification banner may not be appropriate), as well as the contents of the notification message.*> |
| Part b | **Customer Responsibility**  <*The customer will be responsible for displaying the system use notification banner until the user acknowledges the usage condition and takes explicit actions to further access the system. A successful control response will need to address the means by which the user will indicate acknowledgment and move forward.*> |
| Part c | **Customer Responsibility**  <*The customer will be responsible for displaying a system use information message to users. A successful control response will need to address the conditions under which the message will be displayed (if a non-government user accesses the system, the system use information message may not be appropriate), as well as the contents of the notification message, including references to applicable monitoring, recording, or auditing, and authorized usage of the system.*> |

**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.

**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. 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.

| AC-8 | Additional FedRAMP Control Summary Information |
| --- | --- |
| Responsible Role: Customer Administrator, Service Engineer Operations, Security Manager, Azure Program Manager | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| AC-8 What is the solution and how is it implemented? | |
| --- | --- |
| Req. 1 | **Customer Responsibility**  <*The customer will be responsible for determining the conditions under which the system use notification will be displayed. These conditions must be reviewed and accepted by the FedRAMP JAB.*> |
| Req. 2 | **Customer Responsibility**  <*The customer will be responsible for how the system use notification will be verified and how often it should be re-displayed and re-verified. These conditions must be reviewed and accepted by the FedRAMP JAB.*> |
| Req. 3 | **Customer Responsibility**  <*The customer will be responsible for verifying that the system use notification is being displayed as required, either through a configuration baseline check or via other means. If this verification does not happen through a configuration baseline check, the JAB must review and accept the proces used to perform the verification.*> |

* + 1. Concurrent Session Control (AC-10)

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: <*Customer defined account and/or account type; FedRAMP requirement: three sessions for privileged access and two 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| AC-10 What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for limiting the number of concurrent sessions to the customer application as required. A successful control implemented will need to address the technical mechanisms used to enforce this limit.*> |

* + 1. Session Lock (AC-11)

The information system:

1. Prevents further access to the system by initiating a session lock after [*FedRAMP Assignment: fifteen 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 requirement: fifteen 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| AC-11 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  Not applicable. When AC-2(5) is implemented, the non-configurable default behavior of OpenShift is to disconnect idle users from the management console after 15 minutes. |
| Part b | **Customer Responsibility**  Not applicable. When AC-2(5) is implemented, the non-configurable default behavior of OpenShift is to disconnect idle users from the management console after 15 minutes. |

* + - 1. Control Enhancement AC-11 (1)

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

| AC-11 (1) | Control Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| AC-11 (1) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  Not applicable. When AC-2(5) is implemented, the non-configurable default behavior of OpenShift is to disconnect idle users from the management console after 15 minutes. |

* + 1. Session Termination (AC-12)

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*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| AC-12 What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for defining events or conditions requiring disconnection (for example, user requesting logout), and for terminating the session when those events or conditions arise. A successful control response will need to outline the qualifying events or conditions.*> |

* + 1. Permitted Actions without Identification or Authentication (AC-14)

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: Not applicable. | |
| Parameter AC-14(a): Not applicable | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| AC-14 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Non-authenticated users have no access to the system, other than the presentation of the login screen. |

* + 1. Remote Access (AC-17)

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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| AC-17 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for establishing and documenting usage restrictions, configuration and connection requirements, and implementation guidance for access to the customer application (note that in a cloud environment, all user access will be remote access).*> |
| Part b | **Customer Responsibility**  <*The customer will be responsible for authorizing remote access before allowing such connections. Due to the nature of the cloud environment, a successful control response will need to indicate that authorizing remote access is equivalent to authorizing any access, and relate this control to AC-2.*> |

* + - 1. Control Enhancement AC-17 (1)

The information system monitors and controls remote access methods.

| AC-17 (1) | Control Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| AC-17 (1) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  All system events, regardless of local or remote, are captured through the OpenShift and underlying Red Hat Enterprise Linux audit subsystem. This control is inherently met when auditing is enabled. |

* + - 1. Control Enhancement AC-17 (2)

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

| AC-17 (2) | Control Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| AC-17 (2) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  OpenShift uses the following cryptographic algorithms and ciphers to protect confidentiality and integrity of remote access sessions:   * TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256 * TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 * TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384 * TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 * TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA * TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA * TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA * TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA * TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA * TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA * TLS\_ECDHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA * TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA |

* + - 1. Control Enhancement AC-17 (3)

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

| AC-17 (3) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter AC-17(3): <*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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| AC-17 (3) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for requiring remote access connections to the customer application to be routed through customer-defined network access control points. A successful control response will need to address the nature, number, and location of such access control points, as well as the security controls in place to protect those access control points.*> |

* + - 1. Control Enhancement AC-17 (4)

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 Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| AC-17 (4) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for authorizing the execution of privileged commands and access to security-relevant information via remote access. Due to the nature of the cloud environment, a successful control response will need to indicate that authorizing these activities over remote access is equivalent to authorizing them at all, and refer to AC-2.*> |
| Part b | **Customer Responsibility**  <*The customer will be responsible for authorizing the execution of privileged commands and access to security-relevant information via remote access. Due to the nature of the cloud environment, a successful control response will need to indicate that authorizing these activities over remote access is equivalent to authorizing them at all, and refer to AC-2.*> |

* + - 1. Control Enhancement AC-17 (9)

The organization provides the capability to expeditiously disconnect or disable remote access to the information system within [*FedRAMP Assignment: no greater than fifteen minutes*].

| AC-17 (9) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter AC-17(9): <*FedRAMP requirement: no greater than fifteen 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| AC-17 (9) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  OpenShift utilizes the firewall technology embedded into Red Hat Enterprise Linux 7. This technology, named “firewalld”, allows a system administrator to configure host-based rules which take effect immediately. This gives an OpenShift operator the ability to immediately drop all remote connections. For additional information on embedded firewall capabilities, refer to the “Using Firewalls” section of the RHEL7 Security Guide at <https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Security_Guide/sec-Using_Firewalls.html>.  Additionally, OpenShift nodes may be placed into “maintenance mode.” This designation will migrate applications from a given cluster node to another, disconnecting any active sessions to a given cluster node.  If immediate disconnect of all sessions to hosted applications are desired, individual containers may be halted. This will disconnect user sessions for tenant applications. |

* + 1. Wireless Access Restrictions (AC-18)

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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| AC-18 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.1.14. |
| Part b | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.1.14. |

* + - 1. Control Enhancement AC-18 (1)

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

| AC-18 (1) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: Microsoft Azure | |
| Parameter AC-18(1): N/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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| AC-18 (1) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.1.14.1. |

* + 1. Access Control for Portable and Mobile Systems (AC-19)

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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| AC-19 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.1.15. |
| Part b | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.1.15. |

* + - 1. Control Enhancement AC-19 (5)

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 Enhancement Summary Information |
| --- | --- |
| Responsible Role: N/A | |
| Parameter AC-19(5)-1: N/A | |
| Parameter AC-19(5)-2: N/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 (Corporate and System Specific)  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| AC-19 (5) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.1.15.1. |

* + 1. Use of External Information Systems (AC-20)

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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| AC-20 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for establishing terms and conditions allowing authorized individuals to access the customer application from external information systems. A successful control response will need to outline the terms and conditions and the external information systems to which those terms and conditions apply.*> |
| Part b | **Customer Responsibility**  <*The customer will be responsible for establishing terms and conditions allowing authorized individuals to process, store, or transmit customer-controlled information using external information systems. A successful control response will need to outline the terms and conditions and the external information systems to which those terms and conditions apply.*> |

* + - 1. Control Enhancement AC-20 (1)

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 Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| AC-20 (1) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for verifying the implementation of required security controls on external information systems used to access the customer application. A successful control response will need to address how this verification occurs (e.g. through an independent assessment).*> |
| Part b | **Customer Responsibility**  <*If part (a) is not possible, then the customer will be responsible for establishing and retaining approved information system connection or processing agreements with the external entity hosting the external information system used to access the customer application.*> |

* + - 1. Control Enhancement AC-20 (2)

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

| AC-20 (2) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter AC-20(2): <*Customer selection: restricts or prohibits*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| AC-20 (2) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for restricting or prohibiting the use of customer-controlled portable storage devices on external information systems. If such use is not prohibited, a successful control response will need to address specific restrictions on how or under what conditions such use may occur.*> |

* + 1. Information Sharing (AC-21)

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*> | |
| 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| AC-21 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for determining when authorized users are required to use discretion as to whether to share information. A successful control response will need to address the circumstances where user discretion (rather than automatic access enforcement) is required.*> |
| Part b | **Customer Responsibility**  <*The customer will be responsible for defining and employing automated mechanisms or manual processes to assist users in making information sharing decisions.*> |

* + 1. Publicly Accessible Content (AC-22)

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(d): <*FedRAMP requirement: 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| AC-22 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for designating individuals authorized to post information publicly. A successful control response will need to address the specific business requirements or job functions that justify such access.*> |
| Part b | **Customer Responsibility**  <*The customer will be responsible for training designated authorized individuals to prevent disclosure of nonpublic information. A successful control response will need to outline the training provided.*> |
| Part c | **Customer Responsibility**  <*The customer will be responsible for reviewing information prior to public posting to ensure that nonpublic information is not included. A successful control response will need to address the roles or personnel responsible for this review and the process for signoff.*> |
| Part d | **Customer Responsibility**  <*The customer will be responsible for reviewing publicly available information at the required frequency and removing nonpublic information when discovered. A successful control response will need to address the roles or personnel responsible for the review, the process used to review publicly available information, and the process for removal of nonpublic information.*> |

* 1. Awareness and Training (AT)
     1. Security Awareness and Training Policy and Procedures (AT-1)

The organization:

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

| AT-1 | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter AT-1(a): <*Customer-defined personnel or roles*> | |
| Parameter AT-1(b)(1): <*FedRAMP requirement: at least every 3 years*> | |
| Parameter AT-1(b)(2): <*FedRAMP requirement: 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) | |

| AT-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for developing, documenting, and disseminating Security Awareness and Training policy and procedures. A successful control response will need to address the content of the policy (which must include purpose, scope, roles, responsibilities, management commitment, coordination, and compliance) and procedures (which must facilitate the implementation of the policies and associated controls).*> |
| Part b | **Customer Responsibility**  <*The customer will be responsible for reviewing and updating the Security Awareness and Training policy every 3 years, and procedures annually. A successful control response will need to address the review and update process, including the role(s) responsible for initiating the review process, updating the policy and procedures, and providing approval of the updates.*> |

* + 1. Security Awareness (AT-2)

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 requirement: at least annually*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Configured by customer  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| AT-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for providing basic security awareness training as part of initial training. A successful control response will outline the content of the training and will discuss the process for ensuring that all users undergo the required training.*  *Microsoft has created several white papers, case studies, and videos related to security, cloud security, and the secure use of Microsoft services, which customers may use as part of their training program. These resources can be found at* [*https://www.microsoft.com/en-us/TrustCenter/Resources/*](https://www.microsoft.com/en-us/TrustCenter/Security/Identity)*.*> |
| Part b | **Customer Responsibility**  <*The customer will be responsible for providing updated basic security awareness training as required by information system changes. A successful control response will discuss the process for determining what information system changes require updated training, how the training content is updated, and how users are notified of the need for re-training.*> |
| Part c | **Customer Responsibility**  <*The customer will be responsible for refreshing basic security awareness training annually. A successful control response will discuss the process for ensuring that all users undergo the required re-training.*> |

* + - 1. Control Enhancement AT-2 (2)

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

| AT-2 (2) | Control Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| AT-2 (2) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for including information about indicators of insider threat in security awareness training materials. A successful control response will summarize potential indicators of insider threat and outline the process for reporting them to appropriate organizational officials.*> |

* + 1. Role-Based Security Training (AT-3)

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 requirement: at least annually*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| AT-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for providing role-based security training prior to users commencing work on their system. A successful control response will outline the content of the training (including how the content varies by assigned role) and will discuss the process for ensuring that all users undergo the required training for their roles.*> |
| Part b | **Customer Responsibility**  <*The customer will be responsible for providing updated role-based security training as required by information system changes. A successful control response will discuss the process for determining what information system changes require updated training, how the training content is updated, and how users are notified of the need for re-training.*> |
| Part c | **Customer Responsibility**  <*The customer will be responsible for refreshing role-based security training annually. A successful control response will discuss the process for ensuring that all users undergo the required re-training.*> |

* + 1. Security Training Records (AT-4)

The organization:

1. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and
2. Retains individual training records for [*FedRAMP Assignment: at least one year*].

| AT-4 | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter AT-4(b): <*FedRAMP requirement: at least one 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  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| AT-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for tracking successful completion of basic security awareness training and role-based training security training activities. A successful control response will discuss the process or system used to monitor and document completion of training for each user.*> |
| Part b | **Customer Responsibility**  <*The customer will be responsible for retaining training records for the required timeframe. A successful control response will outline the methods by which required retention is achieved.*> |

* 1. Audit and Accountability (AU)
     1. Audit and Accountability Policy and Procedures (AU-1)

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 every three years*]; and
   2. Audit and accountability procedures [*FedRAMP Assignment: at least annually*].

| AU-1 | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter AU-1(a): <*Customer-defined personnel or roles*> | |
| Parameter AU-1(b)(1): <*FedRAMP requirement: at least every 3 years*> | |
| Parameter AU-1(b)(2): <*FedRAMP requirement: 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) | |

| AU-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for developing, documenting, and disseminating Audit and Accountability policy and procedures. A successful control response will need to address the content of the policy (which must include purpose, scope, roles, responsibilities, management commitment, coordination, and compliance) and procedures (which must facilitate the implementation of the policies and associated controls).*> |
| Part b | **Customer Responsibility**  <*The customer will be responsible for reviewing and updating the Audit and Accountability policy every 3 years, and procedures annually. A successful control response will need to address the review and update process, including the role(s) responsible for initiating the review process, updating the policy and procedures, and providing approval of the updates.*> |

* + 1. Audit Events (AU-2)

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 | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter AU-2(a): <*FedRAMP requirement: [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 requirement: [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 Microsoft Azure | |

| AU-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for determining which events their software applications must be capable of auditing. A successful control response will need to address the FedRAMP-required auditable events listed above as well as any additional events the customer feels should be auditable based on customer needs. The following link at the Microsoft Trust Center contains information about how to configure an Azure subscription to enable auditing and logging:* [*https://www.microsoft.com/en-us/trustcenter/security/auditingandlogging*](http://usgcb.nist.gov/usgcb_faq.html)*.*  *Microsoft Azure will audit events at the VM level for PaaS customers; see section 15.3.2.>  <OpenShift, when running on Red Hat Enterprise Linux, utilizes the underlying audit subsystem. When the audit subsystem is enabled, the metadata required by this control is generated>* |
| Part b | Customer Responsibility  *<The customer will be responsible for implementing this control. A successful control response will need to address coordination with all interested parties (such as an internal SOC or security team) and incorporation of their input into business requirements in order to determine the selection of auditable events.>* |
| Part c | Customer Responsibility  *<The customer will be responsible for implementing this control. A successful control response will include a discussion of the decision process behind the selection of auditable events and a justification for the selected events being sufficient to support after-the-fact investigations.>* |
| Part d | Customer Responsibility  *<The customer will be responsible for selecting a subset of the events listed in part a to be audited by the system. For FedRAMP compliance, these events must be monitored continuously. A successful control response will include a discussion of the rationale for the events chosen.*  *The following link at the Microsoft Trust Center contains information about how to configure an Azure subscription to enable auditing and logging:* [*https://www.microsoft.com/en-us/trustcenter/security/auditingandlogging*](https://www.microsoft.com/en-us/TrustCenter/Security/Identity)*.*  *Microsoft Azure will audit events at the VM level for PaaS customers; see section 15.3.2.>*  *<Details on configuring the OpenShift’s underlying audit subsystem can be found here:* <https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Security_Guide/sec-configuring_the_audit_service.html> > |

* + - 1. Control Enhancement AU-2 (3)

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.

| AU-2 (3) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter AU-2(3): <*FedRAMP requirement: annually or whenever there is a change in the threat environment* > | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| AU-2 (3) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  *<Customers are responsible for reviewing and updating the audited events annually or whenever there is a change in the threat environment. A successful control response will outline how often audited events are reviewed.*  *Microsoft Azure will audit events at the VM level for PaaS customers; see section 15.3.2.1.>* |

* + 1. Content of Audit Records (AU-3)

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*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| AU-3 What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  *<Customers are responsible for generating audit records that contain information that establish what type of event occurred, when the even 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. A successful control response will outline what customers require their audit records to contain.*  *Microsoft Azure will audit events at the VM level for PaaS customers; see section 15.3.3.>*  *<OpenShift utilizes the underlying Red Hat Enterprise Linux audit subsystem. Details on configuring the audit subsystem can be found here:* <https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Security_Guide/sec-configuring_the_audit_service.html> > |

* + - 1. Control Enhancement AU-3 (1)

The information system generates audit records containing the following additional information: [*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*]].

**AU-3 (1) Additional FedRAMP Requirements and Guidance:** **Requirement:** The service provider defines audit record types. The audit record types are approved and accepted by the JAB.

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

| AU-3 (1) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter AU-3(1): <*FedRAMP requirement: 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*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| AU-3 (1) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  *<Customers are responsible ensuring that the information generates audit records containing all the information required to meet FedRAMP requirements. A successful control response will outline the system’s audit generation, and the content that it includes.*  *Microsoft Azure will audit events at the VM level for PaaS customers; see section 15.3.3.1.>*  *<Instructions on configuring OpenShift’s underlying audit subsystem can be found here:* [*https://access.redhat.com/documentation/en-US/Red\_Hat\_Enterprise\_Linux/7/html/Security\_Guide/sec-configuring\_the\_audit\_service.html*](https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Security_Guide/sec-configuring_the_audit_service.html) *>* |

* + 1. Audit Storage Capacity (AU-4)

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*> | |
| 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| AU-4 What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  *<Customers are responsible for allocating audit record storage capacity in according with the organizations requirements. A successful control response will explain the procedures in place to ensure that audit storage is allocated according to meet customer requirements. .*  *Microsoft Azure will audit events at the VM level for PaaS customers; see section 15.3.4.>* |

* + 1. Response to Audit Processing Failures (AU-5)

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: low-impact: overwrite oldest audit records; moderate-impact: shut down*].

| AU-5 | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter AU-5(a): <*Customer-defined personnel or roles*> | |
| Parameter AU-5(b): <*FedRAMP requirement: low-impact: overwrite oldest audit records; moderate-impact: shut down* > | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| AU-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  *<Customers are responsible for alerting personnel or roles in the event of an audit processing failure. A successful control response will outline the process taken to alert personnel when an auditing failure occurs.*  *Microsoft Azure will audit events at the VM level for PaaS customers; see section 15.3.5.>*  *<If OpenShift is using the underlying Red Hat Enterprise Linux audit subsystem, instructions for configuring alerting can be found in the Red Hat Enterprise Linux 7 Security Guide:* [*https://access.redhat.com/documentation/en-US/Red\_Hat\_Enterprise\_Linux/7/html/Security\_Guide/sec-configuring\_the\_audit\_service.html*](https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Security_Guide/sec-configuring_the_audit_service.html) *>* |
| Part b | **Customer Responsibility**  *<In the event of an audit processing failure, customers are responsible for: overwriting the oldest audit records for low impact systems and shutting down moderate impact systems. A successful control response will outline the actions taken when an auditing failure occurs.*  *Microsoft Azure will audit events at the VM level for PaaS customers; see section 15.3.5.>*  *<If OpenShift is using the underlying Red Hat Enterprise Linux audit subsystem, instructions for configuring alerting can be found in the Red Hat Enterprise Linux 7 Security Guide:* [*https://access.redhat.com/documentation/en-US/Red\_Hat\_Enterprise\_Linux/7/html/Security\_Guide/sec-configuring\_the\_audit\_service.html*](https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Security_Guide/sec-configuring_the_audit_service.html) *>* |

* + 1. Audit Review, Analysis, and Reporting (AU-6)

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 | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter AU-6(a)-1: <*FedRAMP requirement: at least weekly*> | |
| Parameter AU-6(a)-2: <*Customer defined organization-defined inappropriate or unusual activity* > | |
| Parameter AU-6(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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| AU-6 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  *<Customers are responsible for review and analysis of the information system audit records at least weekly for indications of inappropriate or unusual activity. A successful control response will outline how often audit records are reviewed, and types of activities they are reviewed for.*  *Microsoft Azure will audit events at the VM level for PaaS customers; see section 15.3.6.>* |
| Part b | **Customer Responsibility**  *<Customers are responsible for ensuring that audit review findings are reported to the appropriate personnel. A successful control response will outline how audit review findings are reported.*  *Microsoft Azure will audit events at the VM level for PaaS customers; see section 15.3.6.>* |

* + - 1. Control Enhancement AU-6 (1)

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 Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| AU-6 (1) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  *<Customers are responsible for employing automated mechanisms to integrate audit, review, analysis and reporting process to support organizational processes for investigation and response to suspicious activities. A successful control response will review the automated tools used for integrating review, analysis, and reporting, and how these tools are employed.*  *Microsoft Azure will audit events at the VM level for PaaS customers; see section 15.3.6.1.>* |

* + - 1. Control Enhancement AU-6 (3)

The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.

| AU-6 (3) | Control Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| AU-6 (3) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  *<Customers are responsible for analyzing and correlating audit records across different repositories to gain organizational-wide situational awareness. A successful control response will discuss how the customer correlates and analyzes audit records from different sources. This can include processes and tools used to meet these goals.*  *Microsoft Azure will audit events at the VM level for PaaS customers; see section 15.3.6.2.>* |

* + 1. Audit Reduction and Report Generation (AU-7)

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*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| AU-7 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  *<Customers are responsible for ensuring that the information system provides an audit reduction and report generation capability that supports on demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents. A successful control response will discuss how the information system provides audit reduction and report generation that supports these requirements. This can include a discussion of tools used to provide this capability, and how they are used .*  *Microsoft Azure will audit events at the VM level for PaaS customers; see section 15.3.7.>*  *<OpenShift embeds the Elasticsearch, Fluentd, and Kibana (EFK) stack. This pre-integrated audit reduction capability aggregates logs from nodes and applications running inside your OpenShift Container Platform installation. Once deployed it uses Fluentd to aggregate event logs from all notes, projects, and pods into Elasticsearch (ES). It also provides a centralized Kibana web UI where users and administrators can create rich visualizations and dashboards with the aggregated data. Triggers may be setup to detect atypical use.*  *For aggregate log sizing information, refer to the “Aggregate Logging Sizing Guidelines” of the Installation and Configuration guide:* [*https://docs.openshift.com/container-platform/3.3/install\_config/aggregate\_logging\_sizing.html*](https://docs.openshift.com/container-platform/3.3/install_config/aggregate_logging_sizing.html)    *For instructions on how to configure aggregate logging, refer to the “Aggregating Container Logs” section of the Installation and Configuration guide:* [*https://docs.openshift.com/container-platform/3.3/install\_config/aggregate\_logging.html*](https://docs.openshift.com/container-platform/3.3/install_config/aggregate_logging.html)*>* |
| Part b | **Customer Responsibility**  OpenShift relies upon the underlying Audit Subsystem of Red Hat Enterprise Linux. This audit subsystem has undergone Common Criteria testing, which verifies log integrity during remote transmittal. Certification documents can be found publicly at https://www.redhat.com/en/technologies/industries/government/standards. |

* + - 1. Control Enhancement AU-7 (1)

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 Enhancement Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter AU-7(1): <*Customer 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| AU-7 (1) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  *<Customers are responsible for ensuring that the information system provides the capability to process audit records for events of interest based on defined fields within audit records. A successful control response will discuss how audit records can be queried based on these fields.*  *Microsoft Azure will audit events at the VM level for PaaS customers; see section 15.3.7.1.>  <OpenShift embeds the Elasticsearch, Fluentd, and Kibana (EFK) stack. This pre-integrated audit reduction capability aggregates logs from nodes and applications running inside your OpenShift Container Platform installation. Once deployed it uses Fluentd to aggregate event logs from all notes, projects, and pods into Elasticsearch (ES). It also provides a centralized Kibana web UI where users and administrators can create rich visualizations and dashboards with the aggregated data. Triggers may be setup to detect atypical use.>* |

* + 1. Time Stamps (AU-8)

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: organization-defined granularity of time measurement*].

| AU-8 | Control Summary Information |
| --- | --- |
| Responsible Role: Microsoft Azure Security Engineering Team | |
| Parameter AU-8(b): Millisecond precision | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| AU-8 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  The Linux audit subsystem, upon which OpenShift logs are generated, uses the system clock be default. This is non-configurable behavior. |
| Part b | **Customer Responsibility**  The system time is always kept in Coordinated Universal Time (UTC) and converted in applications to local time as needed. Local time is the actual time on your current time zone, taking into account daylight savings time. The real-time clock can use either UTC or local time. UTC is recommended.  By default, OpenShift hosts are configured to use UTC. To manually ensure this, the timedatectl command may be used:  $ timedatectl set-local-rtc no  Refer to the RHEL7 System Administrators guide for additional information on configuring time on OpenShift nodes: <https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/System_Administrators_Guide/chap-Configuring_the_Date_and_Time.html#sect-Configuring_the_Date_and_Time-timedatectl-Time_Zone> |

* + - 1. Control Enhancement AU-8 (1)

The information system:

1. Compares the internal information system clocks [*FedRAMP Assignment: at least hourly*] with [*FedRAMP Assignment: authoritative time source:* [*http://tf.nist.gov/tf-cgi/servers.cgi*](http://tf.nist.gov/tf-cgi/servers.cgi)]; 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) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter AU-8(1)(a)-1: <*FedRAMP requirement: at least hourly* > | |
| Parameter AU-8(1)(a)-2: <*FedRAMP requirement: authoritative time source:* [*http://tf.nist.gov/tf-cgi/servers.cgi*](https://www.microsoft.com/en-us/TrustCenter/Security/Identity)> | |
| Parameter AU-8(1)(b): <*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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| AU-8(1) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  *<Customers are responsible for comparing the internal information system clocks at least hourly with an authoritative time source. A successful control response will discuss the time source that system clocks are synced with.*  *Microsoft Azure will audit events at the VM level for PaaS customers; see section 15.3.8.1.>* |
| Part b | **Customer Responsibility**  *<Customers are responsible for synchronizing internal system clocks to the authoritative time source when the time difference is greater than the organization has defined. A successful control response will discuss how system clocks are synced.*  *Microsoft Azure will audit events at the VM level for PaaS customers; see section 15.3.8.1.>*  *<OpenShift utilizes the time services of the underlying operating system, Red Hat Enterprise Linux. To configure the network time protocol (NTP) daemon to synchronize against NIST time sources, edit the /etc/ntp.conf file (or create one if it does not exist already). The proper format is:*  *server <<time source>> iburst*  *For detailed NTP configuration, reference the Red Hat Enteprise Linux 7 System Administrators guide:* [*https://access.redhat.com/documentation/en-US/Red\_Hat\_Enterprise\_Linux/7/html/System\_Administrators\_Guide/s1-Configure\_NTP.html*](https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/System_Administrators_Guide/s1-Configure_NTP.html)*>* |

**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) | Additional Control Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| AU-8 (1) What is the solution and how is it implemented? | |
| --- | --- |
| Req. 1 | **Customer Responsibility**  *<Customers are responsible for selecting primary and secondary time servers used by the NIST Internet time services and ensuring that the secondary server is selected from a different region than the primary. A successful control response will discuss which Internet time services are used to by the system.*  *Microsoft Azure will audit events at the VM level for PaaS customers; see section 15.3.8.1.>* |
| Req. 2 | **Customer Responsibility**  *<Customers are responsible for synchronizing the system clocks of network computers that run operating systems other than Windows to the Windows Server Domain Controller emulator, or the same time source for that server. A successful control response will discuss which Internet time services are for non-Windows systems.*  *Microsoft Azure will audit events at the VM level for PaaS customers; see section 15.3.8.1.>* |

* + 1. Protection of Audit Information (AU-9)

The information system protects audit information and audit tools from unauthorized access, modification, and deletion.

| AU-9 | Control Summary Information |
| --- | --- |
| Responsible Role: Microsoft Azure Service Teams, Microsoft Azure Security Engineering Team, Service Engineer Operations | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| AU-9 What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  *<Customers are required to protect the audit information and audit tools from unauthorized access, modification, and deletion. A successful control response will discuss the way that audit information and tools are protected. This can include how access is controlled to audit information and tools.*  *Microsoft Azure will audit events at the VM level for PaaS customers; see section 15.3.9.>  <When running OpenShift on Red Hat Enterprise Linux, configured against the DoD STIG or FISMA profiles, this control is met.>* |

* + - 1. Control Enhancement AU-9 (2)

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 Enhancement Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter AU-9(2): <*FedRAMP requirement: at least weekly* > | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| AU-9 (2) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  *<Customers are required to back up audit records at least weekly to a physically different system or component than the system being audited. A successful control response will discuss the way that audit records are backed up to a system other than the one being audited. This can include a centralized repository for all audit records. .*  *Microsoft Azure will audit events at the VM level for PaaS customers; see section 15.3.9.1.>  <*OpenShift embeds the Elasticsearch, Fluentd, and Kibana (EFK) stack. This pre-integrated audit reduction capability aggregates logs from nodes and applications running inside your OpenShift Container Platform installation. Once deployed it uses Fluentd to aggregate event logs from all notes, projects, and pods into Elasticsearch (ES). It also provides a centralized Kibana web UI where users and administrators can create rich visualizations and dashboards with the aggregated data.> |

* + - 1. Control Enhancement AU-9 (4)

The organization authorizes access to management of audit functionality to only [*Assignment: organization-defined subset of privileged users*].

| AU-9 (4) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter AU-9(4): <*Customer 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| AU-9 (4) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  *<Customers are required to authorize access to management of audit functionality to only a subset of privileged users. A successful control response will discuss how access to audit functionality is restricted to only appropriate personnel. This can include a description of who this functionality is restricted to, and how this is controlled.*  *Microsoft Azure will audit events at the VM level for PaaS customers; see section 15.3.9.2.>* |

* + 1. Audit Record Retention (AU-11)

The organization retains audit records for [*FedRAMP Assignment: at least ninety days*] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

**AU-11 Additional FedRAMP Requirements and Guidance:** Requirement: The service provider retains audit records on-line for at least ninety days and further preserves audit records off-line for a period that is in accordance with NARA requirements

| AU-11 | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter AU-11: <*FedRAMP requirement: at least ninety days* > | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| AU-11 What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  *<Customers are required to retain audit records for at least ninety days to provide support for after the fact investigations of security incidents and to meet regulatory and organizational information retention requirements. A successful control response will discuss how long audit records are retained.*  *Microsoft Azure will audit events at the VM level for PaaS customers; see section 15.3.10.>  <Audit log retention may be configured in the underlying Red Hat Enterprise Linux audit daemon. If using a central or 3rd party logging solution, this may likely need to be configured in that tool.>* |

* + 1. Audit Generation (AU-12)

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*> | |
| Parameter AU-12(a): <*FedRAMP requirement: at least every 3 years*> | |
| 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| AU-12 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  *<Customers are required to provide record generation capability for the events defined in AU-2a at all information systems components where audit capability is available. A successful control response will discuss the configuration of all system components to capture the events that were defined in AU-2.*  *Microsoft Azure will audit events at the VM level for PaaS customers; see section 15.3.11.>*  *<OpenShift logs events through the Red Hat Enterprise Linux 7 Audit subsystem. To verift audit is enabled, run the following command:*  *$ /bin/systemctl status auditd.service*  *The output will indicate the status of the audit daemon.>* |
| Part b | **Customer Responsibility**  *<Customers are required to allow defined personnel or roles to select which auditable events are to be audited by specific components of the information system. A successful control response will discuss how audit generation is implemented, and who selects and configures auditable events on the information system.*  *Microsoft Azure will audit events at the VM level for PaaS customers; see section 15.3.11.>*  *<Audit rules may be added/removed through modifying the /etc/audit/audit.rules or applicable file under /etc/audit/rules.d/. It is recommended that OpenShift specific audit rules be added to /etc/audit/rules.d/openshift.rules.>* |
| Part c | **Customer Responsibility**  *<Customers are required to generate audit records for the events defined in AU-2d with the content defined in AU-3. A successful control response will discuss how audit records are generated, and how they meet the requirements defined in AU-2 and AU-3.*  *Microsoft Azure will audit events at the VM level for PaaS customers; see section 15.3.11.>* |

* 1. Security Assessment and Authorization (CA)
     1. Security Assessment and Authorization Policies and Procedures (CA-1)

The organization:

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

| CA-1 | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter CA-1(a): <*Customer-defined personnel or roles*> | |
| Parameter CA-1(b)(1): <*FedRAMP requirement: at least every 3 years*> | |
| Parameter CA-1(b)(2): <*FedRAMP requirement: 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) | |

| CA-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for developing, documenting, and disseminating Security Assessment and Authorization policy and procedures. A successful control response will need to address the content of the policy (which must include purpose, scope, roles, responsibilities, management commitment, coordination, and compliance) and procedures (which must facilitate the implementation of the policies and associated controls).*> |
| Part b | **Customer Responsibility**  <*The customer will be responsible for reviewing and updating the Security Assessment and Authorization policy every 3 years, and procedures annually. A successful control response will need to address the review and update process, including the role(s) responsible for initiating the review process, updating the policy and procedures, and providing approval of the updates.*> |

* + 1. Security Assessments (CA-2)

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 PMO*].

| CA-2 | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter CA-2(b): <*FedRAMP requirement: at least annually*> | |
| Parameter CA-2(d): <*FedRAMP requirement: individuals or roles to include the FedRAMP 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| CA-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for developing a Security Assessment Plan. A successful control response will need to address the involvement of a FedRAMP-accredited 3PAO (see CA-2(1)), the scope of the assessment, and any specific requirements the customer has for the 3PAO.*> |
| Part b | **Customer Responsibility**  <*The customer will be responsible for assessing the security controls on the customer system at the required frequency. A successful control response will need to address the methodology used to determine the security and compliance posture of the system.*> |
| Part c | **Customer Responsibility**  <*The customer will be responsible for producing a Security Assessment Report as a result of the assessment. A successful control response will need to address the involvement of the 3PAO as well as any specific requirements for the report (e.g., it should include controls that are considered “other than satisfied”, potential weaknesses in controls that meet minimum requirements, recommended remediation steps, and risks associated with the system).*> |
| Part d | **Customer Responsibility**  <*The customer will be responsible for delivering the Security Assessment Report and any supplementary materials to required individuals, including the FedRAMP PMO. A successful control response will need to address the individuals or roles responsible for managing the package for submission and engaging with the PMO.*> |

* + - 1. Control Enhancement CA-2 (1)

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: Must use an accredited 3PAO for JAB authorization.

| CA-2 (1) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter CA-2(1): <*FedRAMP requirement: 3PAO accreditation*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| CA-2 (1) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for employing a FedRAMP-accredited 3PAO to conduct security control assessments. In addition to performing the assessment, this 3PAO will assist in the development of the Security Assessment Plan and Security Assessment Report (see CA-2).>* |

* + - 1. Control Enhancement CA-2 (2)

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 Enhancement Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter CA-2(2)-1: <*FedRAMP requirement: at least annually*> | |
| Parameter CA-2(2)-2: <*FedRAMP requirement: includes announced*> | |
| Parameter CA-2(2)-3: <*FedRAMP requirement: includes vulnerability scanning*> | |
| Parameter CA-2(2)-4: <*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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| CA-2 (2) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for ensuring that, at a minimum, vulnerability scanning is performed annually as a part of the assessment process. A successful control response will need to address the minimum requirement, as well as discussing any additional testing performed during assessments, such as malicious user testing, insider threat assessment, performance/load testing, or other tests the customer chooses to perform.*> |

* + - 1. Control Enhancement CA-2 (3)

The organization accepts the results of an assessment of [*Assignment: organization-defined information system*] performed by [*FedRAMP Assignment: any 3PAO*] when the assessment meets [*FedRAMP Assignment: the conditions of a P-ATO in the FedRAMP Secure Repository*].

| CA-2 (3) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter CA-2(3)-1: <*Customer defined information system*> | |
| Parameter CA-2(3)-2: <*FedRAMP requirement: any 3PAO*> | |
| Parameter CA-2(3)-3: <*FedRAMP requirement: the conditions of a P-ATO in the FedRAMP Secure Repository*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| CA-2 (3) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for working with a 3PAO to assess the system using the methodology prescribed by FedRAMP. A successful control response will need to address how the assessment will be carried out and how the results will be documented and submitted to FedRAMP for approval.*> |

* + 1. System Interconnections (CA-3)

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: 3 years / annually and on input from FedRAMP*].

| System Name | Name of Organization CSP System Connects To | Role and Name of Person Who Signed Connection Agreement | Name and Date of Interconnection Agreement |
| --- | --- | --- | --- |
| <*System connected to*> | <*Owner of connected system*> | <*Contact for connected system*> | <*Name of document and date signed*> |
| <*Brief description of purpose of connection and nature of information communicated*> | | | |
|  |  |  |  |
|  | | | |
|  |  |  |  |
|  | | | |

| CA-3 | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter CA-3(c): <*FedRAMP requirement: 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| CA-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for authorizing connections to external information systems. A successful control response will need to address the individuals or roles responsible for engaging with authorized points of contact for such external systems and the process for documenting and signing the conditions of the connections in Interconnection Security Agreements.*> |
| Part b | **Customer Responsibility**  <*The customer will be responsible for documenting the details of each interconnection. A successful control response will need to address the process for verifying the interface characteristics, security requirements, and the nature of the information communicated; a summary of this information will need to be included as part of the table above.*> |
| Part c | **Customer Responsibility**  <*The customer will be responsible for reviewing and updating the Interconnection Security Agreements at the required frequency. A successful control response will need to discuss the initiation of the review process, as well as the roles or individuals responsible for reviewing, verifying, updating, and approving any changes to the documentation.*> |

* + - 1. Control Enhancement CA-3 (3)

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.

| CA-3 (3) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter CA-3(3)-1: <*Customer defined unclassified, non-national security system*> | |
| Parameter CA-3(3)-2: <*FedRAMP requirement: 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| CA-3 (3) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for requiring unclassified, non-national security systems to connect to customer applications through a TIC. A successful control response will need to address whether this requirement is enforced using technical means or via policy considerations.*> |

* + - 1. Control Enhancement CA-3 (5)

The organization employs [*Selection: allow-all, deny-by-exception; deny-all, permit-by-exception*] policy for allowing [*Assignment: organization-defined information systems]* to connect to external information systems.]

**CA-3 (5) Additional FedRAMP Requirements and Guidance: Guidance:** For JAB Authorization, CSPs shall include details of this control in their Architecture Briefing

| CA-3 (5) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter CA-3(5)-1: <*Customer selection: either allow-all/deny-by-exception or deny-all/permit-by-exception*> | |
| Parameter CA-3(5)-2: <*Customer defined information system (i.e. customer application)*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| CA-3 (5) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for determining whether connections to external information systems will be governed by an allow-all/deny-by-exception policy or by a deny-all/allow-by-exception policy. A successful control response will need to address the rationale for the selection. In addition, the policy choice and its rationale will need to be included in the Architecture Briefing and in the introductory sections of this System Security Plan.*> |

* + 1. Plan of Action and Milestones (CA-5)

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:** POA&Ms must be provided at least monthly.

| CA-5 | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter CA-5(b): <*FedRAMP requirement: at least monthly*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| CA-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for developing a plan of action and milestones (POA&M) for the remediation of any weaknesses or deficiencies discovered during the security assessment. Additionally, any vulnerabilities found as a result of regular vulnerability scanning (see RA-5) must be included in the POA&M reporting. A successful control response will need to discuss the roles or individuals responsible for creating and tracking POA&M items.*> |
| Part b | **Customer Responsibility**  <*The customer will be responsible for updating the POA&M items at the required frequency. A successful control response will need to address the roles or individuals responsible for updating the POA&M items, as well as the process by which POA&M items will be updated and remediated.*> |

* + 1. Security Authorization (CA-6)

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: at least every three years 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. 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 Authorizing Official.

| CA-6 | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter CA-6(c): <*FedRAMP requirement: at least every three years 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| CA-6 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for working with FedRAMP to designate an authorizing official. A successful control response will need to address how an appropriate authorizing official is selected.*> |
| Part b | **Customer Responsibility**  <*The customer will be responsible for receiving official authorization from the authorizing official prior to commencing operations for federal customers. A successful control response will need to address the inputs provided to the authorizing official so that an accreditation decision can be made.*> |
| Part c | **Customer Responsibility**  <*The customer will be responsible for updating the accreditation package at the required frequency. A successful control response will need to address the components of the package that will be updated, the process for re-assessing the system in alignment with the updated package, and the personnel or roles responsible for managing the update process and engaging with FedRAMP for renewal of authorization.*> |

* + 1. Continuous Monitoring (CA-7)

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:** 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 requirement: 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| CA-7 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for developing a continuous monitoring strategy that meets the requirements. For metrics to be monitored, a successful control response will need to include a discussion of what information the customer considers important to monitor, as well as a rationale for that information being sufficient to demonstrate the ongoing security of the system.*> |
| Part b | **Customer Responsibility**  <*The customer will be responsible for developing a continuous monitoring strategy that meets the requirements. For frequency of monitoring, a successful control response will need to address the rationale for the selected frequency. This frequency should be compatible with the frequency of POA&M reporting specified in CA-5.*> |
| Part c | **Customer Responsibility**  <*The customer will be responsible for including ongoing security control assessments as part of the continuous monitoring program. This may include assessment of controls specifically found to be other than satisfied as part of the 3PAO assessments discussed in CA-2, as well as internal assessment of satisfied controls to verify continued effectiveness of implementation. A successful control response will need to address the roles or individuals responsible for testing, as well as the methodology used for testing.* > |
| Part d | **Customer Responsibility**  <*The customer will be responsible for monitoring the metrics defined in part (a) as part of continuous monitoring. A successful control response will need to discuss how metrics are gathered and reported, as well as the conditions under which monitoring will lead to changes or additions to related reporting, such as POA&M reporting.*> |
| Part e | **Customer Responsibility**  <*The customer will be responsible for correlating and analyzing security-related information gathered from multiple sources, including periodic assessments and continuous monitoring. A successful control response will need to address tools or processes used to perform correlation and analysis.*> |
| Part f | **Customer Responsibility**  <*The customer will be responsible for responding appropriately to the results of the analysis in part (e). A successful control response will need to discuss under what conditions each response action should be taken (for example, if a new vulnerability is found in the system, a POA&M item should be opened).*> |
| Part g | **Customer Responsibility**  <*The customer will be responsible for reporting the security status of the system in accordance with FedRAMP requirements at a regular frequency. This frequency should be compatible with the frequency of POA&M reporting specified in CA-5.*> |

**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 | Additional Control Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| CA-7 What is the solution and how is it implemented? | |
| --- | --- |
| Req. 1 | **Customer Responsibility**  <*The customer will be responsible for performing vulnerability scans of operating systems at least monthly. See also RA-5.*> |
| Req. 2 | **Customer Responsibility**  <*The customer will be responsible for performing vulnerability scans of databases and web applications at least monthly. See also RA-5.*> |
| Req. 3 | **Customer Responsibility**  <*The customer will be responsible for ensuring that an independent assessor performs vulnerability scans at least annually. See also CA-2(2).*> |

* + - 1. Control Enhancement CA-7 (1)

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 Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| CA-7 (1) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for monitoring security controls on an ongoing basis with the assistance of an assessment team with a customer-defined level of independence. Note that this may be the 3PAO used for recurring assessments, it may be a different independent assessor, or it may be a team of personnel employed by the customer. A successful control response will need to address the nature of this team and the methods by which they assess security controls within the system.*> |

* + 1. Penetration Testing (CA-8)

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 requirement: 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| CA-8 What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for conducting penetration testing at the required frequency. A successful control response will need to address the systems or components tested and outline the rules of engagement for testing (e.g. operational personnel are/are not notified in advance of testing, certain components of the system are off-limits for this test, etc.).*> |

* + - 1. Control Enhancement CA-8 (1)

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 Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| CA-8 (1) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for employing an independent agent or team to perform penetration testing. A successful control response will need to address how independence is ensured.*> |

* + 1. Internal System Connections (CA-9)

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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| CA-9 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for authorizing connections within the system, such as between two types of virtual machines within the customer environment. A successful control response will need to address the individual or roles with the authorizing responsibility, as well as how a determination is made to allow a connection between components or classes of components.*> |
| Part b | **Customer Responsibility**  <*The customer will be responsible for documenting the required information for each internal connection. This may be documented in e.g. data flow diagrams or architectural diagrams. A successful control response will need to address the process by which this documentation is created.*> |

* 1. Configuration Management (CM)
     1. Configuration Management Policies and Procedures (CM-1)

The organization:

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

| CM-1 | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter CM-1(a): <*Customer-defined personnel or roles*> | |
| Parameter CM-1(b)(1): <*FedRAMP requirement: at least every 3 years*> | |
| Parameter CM-1(b)(2): <*FedRAMP requirement: 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) | |

| CM-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for developing, documenting, and disseminating Configuration Management policy and procedures. A successful control response will need to address the content of the policy (which must include purpose, scope, roles, responsibilities, management commitment, coordination, and compliance) and procedures (which must facilitate the implementation of the policies and associated controls).*> |
| Part b | **Customer Responsibility**  <*The customer will be responsible for reviewing and updating the Configuration Management policy every 3 years, and procedures annually. A successful control response will need to address the review and update process, including the role(s) responsible for initiating the review process, updating the policy and procedures, and providing approval of the updates.*> |

* + 1. Baseline Configuration (CM-2)

The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.

| CM-2 | Control Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| CM-2 What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for developing, documenting, and maintaining configuration control, a current baseline configuration of the information system. A successful control response will need to address the way that baseline configurations are managed and maintained.*> |

* + - 1. Control Enhancement CM-2 (1)

The organization reviews and updates the baseline configuration of the information system:

1. [*FedRAMP Assignment: Annually*];
2. When required due to [*FedRAMP Assignment: when directed by the JAB*]; and
3. As an integral part of information system component installations and upgrades.

| CM-2 (1) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: <*Customer Defined>* | |
| Parameter CM-2(1)(a): <*FedRAMP requirement: at least annually*> | |
| Parameter CM-2(1)(b): <*FedRAMP requirement: 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| CM-2 (1) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for reviewing and updating the baseline configuration of the information system at least annually. A successful control response will need to address how often the baseline configuration is reviewed and updated.*> |
| Part b | **Customer Responsibility**  <*The customer will be responsible for reviewing and updating the baseline configuration of the information system when required by the JAB. A successful control response will need to address updates to the baseline configuration when required by the JAB.*> |
| Part c | **Customer Responsibility**  <*The customer will be responsible for reviewing and updating the baseline configuration of the information system as a part of information system component installations and upgrades. A successful control response will need to address updates to the baseline configuration as a part of installations and upgrades.*> |

* + - 1. Control Enhancement CM-2 (2)

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 Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| CM-2 (2) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for employing automated mechanisms to maintain an up-to-date, completed, accurate, and readily available baseline configuration of the information system. A successful control response will need to address what automated mechanisms are in use to help maintain the baseline configurations of the information system.*> |

* + - 1. Control Enhancement CM-2 (3)

The organization retains [*Assignment*: *organization-defined previous versions of baseline configurations of the information system*] to support rollback.

| CM-2 (3) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter CM-2(3): <*Customer defined previous versions of the baseline configurations*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| CM-2 (3) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for retaining previous versions of baseline configurations to support rollback. A successful control response will need to address how previous versions of baseline configurations will be retained in order to roll back to a previous version.*> |

* + - 1. Control Enhancement CM-2 (7)

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 Enhancement Summary Information |
| --- | --- |
| Responsible Role: Microsoft Azure | |
| Parameter CM-2(7)(a)-1: N/A | |
| Parameter CM-2(7)(a)-2: N/A | |
| Parameter CM-2(7)(b): N/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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| CM-2 (7) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.5.2.4. |
| Part b | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.5.2.4. |

* + 1. Configuration Change Control (CM-3)

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*];
6. Audits and reviews activities associated with configuration-controlled changes to the information system; and
7. 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-3e Additional FedRAMP Requirements and Guidance:** In accordance with record retention policies and procedures.

**CM-3g 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.

| CM-3 | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter CM-3(e): <*Customer defined time period*> | |
| Parameter CM-3(g)-1: <*FedRAMP requirement: CAB*> | |
| Parameter CM-3(g)-2: <*Customer defined*> | |
| Parameter CM-3(g)-3: <*Customer defined*> | |
| Parameter CM-3(g)-4: <*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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| CM-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for determining the types of changes to the information system that are configuration controlled. A successful control response will need to address how decisions are made to determine configuration controlled changes.*> |
| Part b | **Customer Responsibility**  <*The customer will be responsible for reviewing proposed configuration controlled changes to the information system and approving or disapproving changes with explicit consideration for security impact analysis. A successful control response will need to address how decisions are made to approve configuration control changes, including how the security impact of these changes is considered.*> |
| Part c | **Customer Responsibility**  <*The customer will be responsible for documenting configuration change decisions. A successful control response will need to address how configuration change decisions are documented. This can include, for example, what tools are used and what information is documented.*> |
| Part d | **Customer Responsibility**  <*The customer will be responsible for implementing approved configuration-controlled changes to the system. A successful control response will need to address how changes are implemented after being approved. This can include tools used ensure that changes are implemented after approval.*> |
| Part e | **Customer Responsibility**  <*The customer will be responsible for retaining records of configuration-controlled changes to the information system for a defined period. A successful control response will need to address long records of configuration-controlled changes are kept, and where these records are maintained.*> |
| Part f | **Customer Responsibility**  <*The customer will be responsible for auditing and reviewing activities associated with configuration-controlled changes to the information system for a defined period. A successful control response will need to configuration control changes activities are audited and reviewed. This can include tools used to track these changes and when these changes are reviewed.*> |
| Part g | **Customer Responsibility**  <*The customer will be responsible for coordinating and providing oversight for the configuration control activities through a central means of communicating major changes or developments that may affect services to the federal government. The means of communication must be approved and accepted by the JAB. A successful control response will outline how major changes or developments that affect government services will be coordinated and overseen.*> |

* + 1. Security Impact Analysis (CM-4)

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*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| CM-4 What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for analyzing changes to the information system to determine potential security impacts prior to change implementation. A successful control response will explain the process used to analyze changes before their implementation. This can include any analysis and testing done prior to implementation.>* |

* + 1. Access Restrictions for Change (CM-5)

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*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| CM-5 What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for defining, documenting, approving and enforcing physical and logical access restrictions associated with changes to the information system. A successful control response will include how logical access associated with change control is defined, documented, and enforced. This should include tools used to enforce these restrictions, such as Active Directory, and how these personnel are approved for access.*> |

* + - 1. Control Enhancement CM-5 (1)

The information system enforces access restrictions and supports auditing of the enforcement actions.

| CM-5 (1) | Control Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| CM-5 (1) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for enforcing access restrictions, and supporting auditing of the enforcement actions. A successful control response will explain how access restrictions are enforced, and how this access is audited.*> |

* + - 1. Control Enhancement CM-5 (3)

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:** If digital signatures/certificates are unavailable, alternative cryptographic integrity checks (hashes, self-signed certs, etc.) can be used.

| CM-5 (3) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter CM-5(3): <*Customer defined software*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| CM-5 (3) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  *<To ensure the system can cryptographically verify base software packages of the operating system and OpenShift, the yum “gpgcheck” option must be enabled. This is accomplished by applying the following Red Hat CCes:*   * *CCE-26989-4: Ensure gpgcheck Enabled in Main Yum Configuration* * *CCE-26957-1: Ensure Red Hat GPG Key Installed* * *CCE-26876-3: Ensure gpgcheck Enabled for All Yum Package Repositories* * *CCE-80347-8: Ensure gpgcheck Enabled for Local Packages* * *CCE-80348-6: Ensure gpgcheck Enabled for Repository Metadata>*   *<* |

* + - 1. Control Enhancement CM-5 (5)

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 Enhancement Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter CM-5(5)(b): <*FedRAMP requirement: 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| CM-5 (5) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for limiting privileges to change information system components and system related information within a production or operational environment. A successful control response will include how privileges to change the production/operation environment are limited. This can include defining who has access to these privileges, how they may be separated, and any gates they must go through.*> |
| Part b | **Customer Responsibility**  <*The customer will be responsible for reviewing and reevaluating privileges at least quarterly. A successful control response will include how often reviews are performed for personnel with privileges to change the information system within the production environment.*> |

* + 1. Configuration Settings (CM-6)

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.

**Requirement 2:** The service provider shall ensure that checklists for configuration settings are Security Content Automation Protocol (SCAP) validated or SCAP compatible (if validated checklists are not available).

**Guidance:** Information on the USGCB checklists can be found at: [http://usgcb.nist.gov/usgcb\_faq.html#usgcbfaq\_usgcbfdcc](https://www.microsoft.com/en-us/TrustCenter/Resources/#usgcbfaq_usgcbfdcc).

1. Implements the configuration settings;
2. 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
3. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

**Note:** Information on the USGCB checklists can be found at: [*http://usgcb.nist.gov/usgcb\_faq.html#usgcbfaq\_usgcbfdcc\*](http://tf.nist.gov/tf-cgi/servers.cgi#usgcbfaq_usgcbfdcc\)

Information on SCAP can be found at:[*http://scap.nist.gov/*](http://tf.nist.gov/tf-cgi/servers.cgi)

| CM-6 | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter CM-6(a): <*FedRAMP requirement: see guidance*> | |
| 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| CM-6 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for establishing and documenting configuration settings for information technology products employed within the information system using FedRAMP guidance that reflects the most restrictive mode consistent with operational requirements. A successful control response will include how the customer develops base configurations to ensure that they are as restrictive as possible while still allowing the system to operate.*> |
| Part b | **Customer Responsibility**  <*The customer will be responsible for implementing configuration settings. A successful control response will describe how mandatory configuration settings are implemented. This can include the process or documentation followed.*> |
| Part c | **Customer Responsibility**  <*The customer will be responsible for identifying, documenting, and approving any deviations from established configuration settings for components based on operational requirements. A successful control response will explain the process for identifying documenting, and approving any deviations. This can include tools used to track any exceptions, and the processes for identifying and approving these deviations.*> |
| Part d | **Customer Responsibility**  <*The customer will be responsible for monitoring and controlling changes to the configuration settings in accordance with organization policies and procedures. A successful control response will describe how changes are controlled and monitored. This can include limitations to privileges, how these changes are audited, and any tools in place to track and approve changes.*> |

* + - 1. Control Enhancement CM-6 (1)

The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings for [*Assignment: organization-defined information system components*].

| CM-6 (1) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| CM-6 (1) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for employing automated mechanisms to centrally manage, apply, and verify configuration settings for information system components. A successful control response will describe any automated systems in place used to manage, apply, and verify configuration settings. An example of this is using Active Directory Group Policy Objects to manage security settings.*>  *<From an OpenShift perspective, Ansible playbooks are used to automate deployment and configuration.>* |

* + 1. Least Functionality (CM-7)

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.

**Guidance:** Information on the USGCB checklists can be found at: [http://usgcb.nist.gov/usgcb\_faq.html#usgcbfaq\_usgcbfdcc](https://azure.microsoft.com/en-us/documentation/articles/active-directory-hybrid-identity-design-considerations-overview/#usgcbfaq_usgcbfdcc).

| CM-7 | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter CM-7(b): <*FedRAMP requirement: See FedRAMP 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

|  |  |
| --- | --- |
| CM-7 What is the solution and how is it implemented? | |
| Part a | **Customer Responsibility**  <*The customer will be responsible for configuring the information system to only provide essential capabilities. A successful control response will describe the process used to ensure that information systems only provide essential capabilities. This can include such things as using USGCB guidance and CIS Benchmarks to help ensure that only essential functions are provided.*> |
| Part b | **Customer Responsibility**  <*The customer will be responsible for prohibiting or restricting the use of functions, ports, protocols, and/or services following the USGCB guidance. A successful control response will describe the process used determine functions, ports, protocols, and services to restrict or prohibit, using USGCB guidance.*> |

* + - 1. Control Enhancement CM-7 (1)

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 Enhancement Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter CM-7(1)(a): <*FedRAMP requirement: 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| CM-7 (1) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for reviewing the information system at least monthly to identify unnecessary or nonsecure functions, ports, protocols, and services. A successful control response will describe how often functions, ports, protocols, and services are reviewed.>* |
| Part b | **Customer Responsibility**  <*The customer will be responsible for disabling functions, ports, protocols, and services that have been deemed to be unnecessary or nonsecure. A successful control response will explain that these functions, ports, protocols, and services found during the review process are disabled.*> |

* + - 1. Control Enhancement CM-7 (2)

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 Enhancement Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter CM-7(2): <*Customer defined policies regarding software program usage or 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| CM-7 (2) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for preventing program execution in accordance with organizational defined policies regarding software program usage and restrictions. A successful control response will explain the process used to ensure that policies followed. This can include processes used to detect unauthorized software, or any whitelisting used.*>  <OpenShift utilizes trusted container registries to house ‘white listed’ container images. The organization should define processes for managing said trusted registries to satisfy this control.> |

* + - 1. Control Enhancement CM-7 (5)

The organization:

1. Identifies [*Assignment: organization-defined software programs authorized to execute on the information system*];
2. Employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the information system; and
3. Reviews and updates the list of authorized software programs [*FedRAMP Assignment: at least annually or when there is a change.*].

| CM-7 (5) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter CM-7(5)(a): <*Customer defined software programs authorized to execute on the information system*> | |
| Parameter CM-7(5)(c): <*FedRAMP requirement: at least annually*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| CM-7 (5) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for identifying software programs authorized to execute on the information system. A successful control response will explain the process used to identify authorized software programs.*>  *<Red Hat container image signing provides a path to ensure authorship, integrity and nonrepudiation. Refer to the ‘Container Image Signing Integration Guide’ for procedures on how to setup and maintain container signing:* <https://access.redhat.com/articles/2750891>> |
| Part b | **Customer Responsibility**  <*The customer will be responsible for employing a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the information system. A successful control response will explain the process to allow the execution of software on the information system.*>  *<Red Hat container image signing provides a path to ensure authorship, integrity and nonrepudiation. Refer to the ‘Container Image Signing Integration Guide’ for procedures on how to setup and maintain container signing:* <https://access.redhat.com/articles/2750891>> |
| Part c | **Customer Responsibility**  <*The customer will be responsible for reviewing and updating the list of authorized software programs at least annually or when there is a change. A successful control response will outline how often the authorized software list is reviewed and updated. This should be done at least annually and when changes are made.*>  *<Red Hat container image signing provides a path to ensure authorship, integrity and nonrepudiation. Refer to the ‘Container Image Signing Integration Guide’ for procedures on how to setup and maintain container signing:* <https://access.redhat.com/articles/2750891>> |

* + 1. Information System Component Inventory (CM-8)

The organization:

1. Develops and documents an inventory of information system components that:
   1. Accurately reflects the current information system;
   2. Includes all components within the authorization boundary of the information system;
   3. Is at the level of granularity deemed necessary for tracking and reporting; and
   4. Includes [*Assignment: organization-defined information deemed necessary to achieve effective information system component accountability*]; and
2. 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*> | |
| Parameter CM-8(a)(4): <*Customer defined information deemed necessary to achieve effective information system component accountability*> | |
| Parameter CM-8(b): <*FedRAMP requirement: at least monthly*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| CM-8 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for developing and documenting an inventory that meets FedRAMP requirements. A successful control response will include a description of how the inventory is developed and documented. This process should ensure that the inventory accurate reflects the current system, includes and components, is granular enough to support tracking and reporting, and includes any information the customer has deemed necessary to achieve effective accountability.*> |
| Part b | **Customer Responsibility**  <*The customer will responsible for reviewing and updating the system inventory at least monthly. This may be performed in conjunction with continuous monitoring and POA&M tracking activities. A successful control response will need to address the personnel or roles responsible for updating the system inventory and the process for correcting gaps or discrepancies found.* |

* + - 1. Control Enhancement CM-8 (1)

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.*

| CM-8 (1) | Control Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| CM-8 (1) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible updating the inventory of information system components and an integral part of installations, removals, and information system updates. A successful control response will include a description of how the inventory is updated when any of the above events change the inventory.*> |

* + - 1. Control Enhancement CM-8 (3)

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 Enhancement Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter CM-8(3)(a): <*FedRAMP requirement: Continuously, using automated mechanisms with a maximum five-minute delay in detection* > | |
| Parameter CM-8(3)(b): <*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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| CM-8 (3) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for employing automated mechanisms continuous to detect the presence of unauthorized software within the information system. A successful control response will describe automated systems that are in place to detect unauthorized software on the information system.*> |
| Part b | **Customer Responsibility**  <*The customer will be responsible for actions taken when unauthorized software is detected. A successful control response will describe the actions taken when unauthorized software is detected. This can include notifying personnel, isolating the system, and disabling network access to that system.*> |

* + - 1. Control Enhancement CM-8 (5)

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 Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| CM-8 (5) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible verifying all components within the authorization boundary of the information system are not duplicated in other information system inventories. A successful control response will describe the process used to ensure that assets are not included in multiple system inventories.*> |

* + 1. Configuration Management Plan (CM-9)

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 from unauthorized disclosure and modification.

| CM-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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| CM-9 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for developing, documenting, and implementing a configuration management plan that addresses roles, responsibilities, and configuration management processes and procedures. A successful control response will describe how the configuration management plan deals with roles, responsibilities, and processes and procedures.*> |
| Part b | **Customer Responsibility**  <*The customer will be responsible for developing, documenting, and implementing a configuration management plan that establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of configuration items. A successful control response will describe how the configuration management plan establishes a system to track and manage changes to the system.*> |
| Part c | **Customer Responsibility**  <*The customer will be responsible for developing, documenting, and implementing a configuration management plan that defines the configuration items for the information system and places them under configuration management. A successful control response will describe how the configuration management plan defines configuration items, and the processes used to manage them.*> |
| Part d | **Customer Responsibility**  <*The customer will be responsible for developing, documenting, and implementing a configuration management plan that protects the configuration management plan from unauthorized disclosure. A successful control response will describe how the configuration management plan is protected from disclosure, such as where it is stored, and controls in place to prevent unauthorized access.*> |

* + 1. Software Usage Restrictions (CM-10)

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*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| CM-10 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for using software and associated documentation in accordance with contract agreements and copyright laws. A successful control response will include a description or reference to the customer’s acceptable use policy.*> |
| Part b | **Customer Responsibility**  <*The customer will be responsible for tracking the use of software and associated documentation protected by quantity licenses to control copying and distribution. A successful control response will include a description of how these licenses are tracked and protected.*> |
| Part c | **Customer Responsibility**  <*The customer will be responsible for control and documentation of 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. A successful control response will include any controls and documentation for peer-to-peer technology allowed within the system. An example of this could include acceptable use policies in place.*> |

* + - 1. Control Enhancement CM-10 (1)

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*> | |
| 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| CM-10(1) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for establishing any restrictions on the use of open source software. A successful control response will describe any restrictions that the organization has in place.*> |

* + 1. User Installed Software (CM-11)

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 at [*FedRAMP* *Assignment: Continuously (via CM-7 (5))*].

| CM-11 | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter CM-11(a): <*Customer defined policies*> | |
| Parameter CM-11(b): <*Customer defined methods*> | |
| Parameter CM-11(c): <*FedRAMP requirement: 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| CM-11 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for establishing policies governing the installation of software by users. A successful control response will describe policies in place that define the restrictions in place for installation of software by users.*> |
| Part b | **Customer Responsibility**  <*The customer will be responsible for enforcing installation policies using a defined method. A successful control response will describe the process used to enforce installation policies. This can include references to configuration control processes.*> |
| Part c | **Customer Responsibility**  <*The customer will be responsible for monitoring compliance continuously. A successful control response will describe the process used to monitor compliance of installation policies.*> |

* 1. Contingency Planning (CP)
     1. Contingency Planning Policy and Procedures (CP-1)

The organization:

1. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:
   1. A contingency 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 contingency planning policy and associated contingency planning controls; and
2. Reviews and updates the current:
   1. Contingency planning policy [*FedRAMP Assignment: at least every three years*]; and
   2. Contingency planning procedures [*FedRAMP Assignment: at least annually*].

| CP-1 | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter CP-1(a): <*Customer-defined personnel or roles*> | |
| Parameter CP-1(b)(1): <*FedRAMP requirement: at least every 3 years*> | |
| Parameter CP-1(b)(2): <*FedRAMP requirement: 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) | |

| CP-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for developing, documenting, and disseminating Contingency Planning policy and procedures. A successful control response will need to address the content of the policy (which must include purpose, scope, roles, responsibilities, management commitment, coordination, and compliance) and procedures (which must facilitate the implementation of the policies and associated controls).*> |
| Part b | **Customer Responsibility**  <*The customer will be responsible for reviewing and updating the Contingency Planning policy every 3 years, and procedures annually. A successful control response will need to address the review and update process, including the role(s) responsible for initiating the review process, updating the policy and procedures, and providing approval of the updates.*> |

* + 1. Contingency Plan (CP-2)

The organization:

1. Develops a contingency plan for the information system that:
   1. Identifies essential missions and business functions and associated contingency requirements;
   2. Provides recovery objectives, restoration priorities, and metrics;
   3. Addresses contingency roles, responsibilities, assigned individuals with contact information;
   4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;
   5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and
   6. Is reviewed and approved by [*Assignment: organization-defined personnel or roles*];
2. Distributes copies of the contingency plan to [*Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements*];
3. Coordinates contingency planning activities with incident handling activities;
4. Reviews the contingency plan for the information system [*FedRAMP Assignment: at least annually*];
5. Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;
6. Communicates contingency plan changes to [*Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements*]; and
7. Protects the contingency plan from unauthorized disclosure and modification.

**CP-2 Additional FedRAMP Parameter 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 contingency personnel*> | |
| Parameter CP-2(d): <*FedRAMP requirement: at least annually*> | |
| Parameter CP-2(f): <*Customer defined contingency personnel*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| CP-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for developing a contingency plan meeting the specified requirements. A successful control response will need to address the maintenance, recovery, and resumption of customer applications, as well as any reliance on Microsoft Azure functionality to perform these tasks.*  *Microsoft Azure has provided Site Recovery documentation to assist in creation of contingency plans and contingency plan materials:* [*https://azure.microsoft.com/en-us/documentation/learning-paths/site-recovery/*](https://azure.microsoft.com/en-us/documentation/learning-paths/site-recovery/)*.*> |
| Part b | **Customer Responsibility**  <*The customer will be responsible for distributing the contingency plan to key contingency personnel. A successful control response will need to address identification of key personnel (by name, title, or role) and the means by which the customer ensures that all key personnel receive the contingency plan.*> |
| Part c | **Customer Responsibility**  <*The customer will be responsible for coordinating contingency planning activities with incident handling activities. A successful control response will need to address the division of responsibilities between contingency personnel and incident response personnel, as well as the means by which contingency planning activities are activated in the event of a security incident.*> |
| Part d | **Customer Responsibility**  <*The customer will be responsible for reviewing the contingency plan at the required frequency. A successful control response will need to outline how reviews are initiated, performed, and signed off on.*> |
| Part e | **Customer Responsibility**  <*The customer will be responsible for updating the contingency plan to address relevant changes as well as any problems found in the contingency plan. A successful control response will need to discuss how updates are proposed, implemented, and approved.*> |
| Part f | **Customer Responsibility**  <*The customer will be responsible for communicating changes to the contingency plan to key contingency personnel. A successful control response will need to address the means by which the customer ensures that all key personnel receive the updated contingency plan.*> |
| Part g | **Customer Responsibility**  <*The customer will be responsible for protecting the contingency plan from unauthorized disclosure or modification. A successful control response will need to address policy, procedural, and technical safeguards that are in place to protect the contingency plan.*> |

* + - 1. Control Enhancement CP-2 (1)

The organization coordinates contingency plan development with organizational elements responsible for related plans.

| CP-2 (1) | Control Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| CP-2 (1) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for coordinating development of the contingency plan with related plans (such as business continuity plans, disaster recovery plans, etc.). A successful control response will need to address the coordination of initial development, as well as how updates to the contingency plan affect related plans and vice versa.*> |

* + - 1. Control Enhancement CP-2 (2)

The organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.

| CP-2 (2) | Control Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| CP-2 (2) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  *<The customer will be responsible for reserving capacity for processing in an alternate region, for the following:*   * *Azure Core - Cloud Services (Web and Worker Roles), IaaS/VMs, WA Task, Service Bus, Storage (tables, blobs, queues)*   *A successful control response will need to note that capacity for necessary processing has been reserved in an alternate region, and will then indicate inheritance of capacity planning from Microsoft Azure.>*  **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers (as long as those customers have reserved capacity in an alternate region). See section 14.6.2.2. |

* + - 1. Control Enhancement CP-2 (3)

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 Enhancement Summary Information |
| --- | --- |
| Responsible Role: Microsoft Azure | |
| Parameter CP-2(3): Recovery Time Objectives documented 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| CP-2 (3) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.6.2.3. |

* + - 1. Control Enhancement CP-2 (8)

The organization identifies critical information system assets supporting essential missions and business functions.

| CP-2 (8) | Control Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| CP-2 (8) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  *<The customer will be responsible for identifying critical functionality for which processing capacity must be reserved in an alternate region. A successful control response will need to discuss the process by which this determination is made. Once processing capacity is reserved in an alternate region for this critical functionality, the remainder of the control may be inherited from Microsoft Azure.>*  **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.6.2.4. |

* + 1. Contingency Training (CP-3)

The organization provides contingency training to information system users consistent with assigned roles and responsibilities:

1. Within [*FedRAMP Assignment: 10 days*] of assuming a contingency role or responsibility;
2. When required by information system changes; and
3. [*FedRAMP Assignment: at least annually*] thereafter

| CP-3 | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter CP-3(a): <*FedRAMP requirement: 10 days*> | |
| Parameter CP-3(c): <*FedRAMP requirement: at least annually*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| CP-3 What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  *<The customer will be responsible for initial and refresher training related to contingency plan activities at the required intervals. A successful control response will need to outline the scope and contents of the training, the audience for the training, and the means by which training attendance is tracked and enforced.>* |

* + 1. Contingency Plan Testing (CP-4)

The organization:

1. Tests the contingency plan for the information system [*FedRAMP Assignment: at least annually for moderate impact systems; at least every three years for low impact systems*] using [*FedRAMP Assignment: functional exercises for moderate impact systems; classroom exercises/table top written tests for low impact systems*] 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 Authorizing Official prior to initiating testing.

1. Reviews the contingency plan test results; and
2. Initiates corrective actions, if needed.

| CP-4 | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter CP-4(a)-1: <*FedRAMP requirement: at least annually*> | |
| Parameter CP-4(a)-2: <*FedRAMP requirement: functional exercises for moderate impact systems; classroom exercises/table top written tests for low impact systems*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| CP-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  *<The customer will be responsible for testing of contingency plans related to the customer application at the required frequency. A successful control response will need to address the scenarios and exercises chosen for the test.*  *Microsoft Azure has provided documentation around recovery testing for Azure SQL Database, which customers may use to develop their own test plans and procedures:* [*https://azure.microsoft.com/en-us/documentation/articles/sql-database-disaster-recovery-drills/*](https://www.microsoft.com/en-us/trustcenter/security/auditingandlogging)*.>* |
| Part b | **Customer Responsibility**  *<The customer will be responsible for reviewing the results of contingency plan testing. A successful control response will need to discuss the roles or personnel responsible for review, as well as the format and content of reporting on the results.>* |
| Part c | **Customer Responsibility**  *<The customer will be responsible for initiating corrective action as a result of contingency plan testing. A successful control response will need to address the types of corrective actions taken and timeframes for those actions.>* |

* + - 1. Control Enhancement CP-4 (1)

The organization coordinates contingency plan testing and/or exercises with organizational elements responsible for related plans.

| CP-4 (1) | Control Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| CP-4 (1) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for coordinating testing of the contingency plan with related plans (such as business continuity plans, disaster recovery plans, etc.). A successful control response will need to address ensuring that any test results relevant to related plans are communicated so that corrective actions may be taken as needed.*> |

* + 1. Alternate Storage Site (CP-6)

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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| CP-6 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  *<The customer will be responsible for enabling geo-replicated backups within their subscriptions, which will allow restoration from backup as discussed here:* [*http://msdn.microsoft.com/en-us/library/azure/dn715779.aspx*](https://technet.microsoft.com/en-us/magazine/dn250023.aspx)*. Once geo-replicated backups are enabled, the customer may inherit the remainder of this control from Microsoft Azure.>*  **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers (as long as those customers have enabled geo-replicated backups). See section 14.6.5. |
| Part b | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers (as long as those customers have enabled geo-replicated backups). See section 14.6.5. |

* + - 1. Control Enhancement CP-6 (1)

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 Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| CP-6 (1) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers (as long as those customers have enabled geo-replicated backups). See section 14.6.5.1. |

* + - 1. Control Enhancement CP-6 (3)

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 Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| CP-6 (3) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers (as long as those customers have enabled geo-replicated backups). See section 14.6.5.2. |

* + 1. Alternate Processing Site (CP-7)

The organization:

1. Establishes an alternate processing site including necessary agreements to permit the transfer and resumption of [*Assignment: organization-defined information system operations*] for essential missions/business functions within [*FedRAMP Assignment: See additional FedRAMP requirements and guidance*] when the primary processing capabilities are unavailable;

**CP-7a Additional FedRAMP Requirements and Guidance: Requirement:** The service provider defines a time period consistent with the recovery time objectives and business impact analysis.

1. Ensures that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the organization-defined time period for transfer/resumption; and
2. Ensures that the alternate processing site provides information security safeguards equivalent to that of the primary site.

| CP-7 | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*>, Microsoft Azure | |
| Parameter CP-7(a)-1: <*Customer defined operations*>, operations defined in Microsoft Azure BCPs | |
| Parameter CP-7(a)-2: recovery time defined 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| CP-7 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  *<The customer will be responsible for reserving capacity for processing in an alternate region, for the following:*   * *Azure Core - Cloud Services (Web and Worker Roles), IaaS/VMs, WA Task, Service Bus, Storage (tables, blobs, queues)*   *A successful control response will need to note that capacity for necessary processing has been reserved in an alternate region, and will then indicate inheritance of capacity planning from Microsoft Azure.>*  **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers (as long as those customers have reserved capacity in an alternate region). See section 14.6.6. |
| Part b | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers (as long as those customers have reserved capacity in an alternate region). See section 14.6.6. |
| Part c | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers (as long as those customers have reserved capacity in an alternate region). See section 14.6.6. |

* + - 1. Control Enhancement CP-7 (1)

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:** 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 Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| CP-7 (1) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers (as long as those customers have reserved capacity in an alternate region). See section 14.6.6.1. |

* + - 1. Control Enhancement CP-7 (2)

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 Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| CP-7 (2) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers (as long as those customers have reserved capacity in an alternate region). See section 14.6.6.2. |

* + - 1. Control Enhancement CP-7 (3)

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 Enhancement Summary Information |
| --- | --- |
| Responsible Role: Microsoft Azure | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Configured by customer  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| CP-7 (3) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers (as long as those customers have reserved capacity in an alternate region). See section 14.6.6.3. |

* + 1. Telecommunications Services (CP-8)

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 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  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| CP-8 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers (as long as those customers have reserved capacity in an alternate region). See section 14.6.7. |

* + - 1. Control Enhancement CP-8 (1)

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 Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| CP-8 (1) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers (as long as those customers have reserved capacity in an alternate region). See section 14.6.7.1. |
| Part b | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers (as long as those customers have reserved capacity in an alternate region). See section 14.6.7.1. |

* + - 1. Control Enhancement CP-8 (2)

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 Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| CP-8 (2) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers (as long as those customers have reserved capacity in an alternate region). See section 14.6.7.2. |

* + 1. Information System Backup (CP-9)

The organization:

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) or provides an equivalent alternative. The backup storage capability is approved and accepted by the JAB.

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) or provides an equivalent alternative. The backup storage capability is approved and accepted by the JAB.

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) or provides an equivalent alternative. The backup storage capability is approved and accepted by the JAB

1. Protects the confidentiality, integrity, and availability of backup information at storage locations.

**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.

Requirement: The service provider shall determine how Information System Backup is going to be verified and appropriate periodicity of the check.

| CP-9 | Control Summary Information |
| --- | --- |
| Responsible Role: Microsoft Azure | |
| CP-9a Parameter 1: Daily incremental; weekly full | |
| CP-9b Parameter 1: Daily incremental; weekly full | |
| CP-9c Parameter 1: 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| CP-9 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.6.8. |
| Part b | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.6.8. |
| Part c | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.6.8. |
| Part d | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.6.8. |

* + - 1. Control Enhancement CP-9 (1)

The organization tests backup information [*FedRAMP Assignment: at least annually*] to verify media reliability and information integrity.

| CP-9 (1) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: Microsoft Azure | |
| CP-9(1) Parameter 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| CP-9 (1) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.6.8.1. |

* + - 1. Control Enhancement CP-9 (3)

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 Enhancement Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*>, Microsoft Azure | |
| Parameter CP-9(3): <*Customer data backed up using geo-replication*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| CP-9 (3) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  *<The customer will be responsible for enabling geo-replicated backups within their subscriptions, which will allow restoration from backup as discussed here:* [*http://msdn.microsoft.com/en-us/library/azure/dn715779.aspx*](http://scap.nist.gov/)*. Once geo-replicated backups are enabled, the customer may inherit the remainder of this control from Microsoft Azure.>*  **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers (as long as those customers have enabled geo-replicated backups). See section 14.6.8.2. |

* + 1. Information System Recovery and Reconstitution (CP-10)

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: 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| CP-10 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.6.9. |

* + - 1. Control Enhancement CP-10 (2)

The information system implements transaction recovery for systems that are transaction-based.

| CP-10 (2) | Control Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| CP-10 (2) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  *<The customer will be responsible for implementing transaction recovery within the customer application. A successful control response will need to address how transactions are performed and what occurs in the case of failed or conflicting transactions.>* |

* 1. Identification and Authentication (IA)
     1. Identification and Authentication Policy and Procedures (IA-1)

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 [*Assignment: at least every 3 years*]; and
   2. Identification and authentication procedures [*Assignment: at least annually*].

|  |  |
| --- | --- |
| IA-1 | Control Summary Information |
| Responsible Role: <*Customer defined*> | |
| Parameter IA-1(a): <*Customer-defined personnel or roles*> | |
| Parameter IA-1(b)(1): <*FedRAMP requirement: at least every 3 years*> | |
| Parameter IA-1(b)(2): <*FedRAMP requirement: 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) | |

| IA-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for developing, documenting, and disseminating Identification and Authentication policy and procedures. A successful control response will need to address the content of the policy (which must include purpose, scope, roles, responsibilities, management commitment, coordination, and compliance) and procedures (which must facilitate the implementation of the policies and associated controls).*> |
| Part b | **Customer Responsibility**  <*The customer will be responsible for reviewing and updating the Identification and Authentication policy every 3 years, and procedures annually. A successful control response will need to address the review and update process, including the role(s) responsible for initiating the review process, updating the policy and procedures, and providing approval of the updates.*> |

* + 1. User Identification and Authentication (IA-2)

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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| IA-2 What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for uniquely identifying and authenticating organizational users. Microsoft Azure Active Directory may be used for this purpose. A successful control response will need to address the credentials used to identify and authenticate users, both internal and external if applicable.*  *Microsoft’s Trust Center has resources related to identity and access management. For example:*   * [*https://www.microsoft.com/en-us/TrustCenter/Security/Identity*](http://usgcb.nist.gov/usgcb_faq.html) *discusses the use of Azure Active Directory (AAD) and Azure Multi-Factor Authentication to manage customer access* * [*https://azure.microsoft.com/en-us/documentation/articles/multi-factor-authentication-security-best-practices/*](https://azure.microsoft.com/en-us/documentation/articles/multi-factor-authentication-security-best-practices/) *addresses the use of Multi-Factor Authentication in more detail* * [*https://azure.microsoft.com/en-us/documentation/articles/active-directory-hybrid-identity-design-considerations-overview/*](https://azure.microsoft.com/en-us/documentation/articles/sql-database-disaster-recovery-drills/) *addresses the integration of cloud-based identity management with existing on-premises identity management solutions*>   *<As an OpenShift Container Platform administrator, you can use groups to manage users, change their permissions, and enhance collaboration. Your organization may have already created user groups and stored them in an LDAP server, such as Active Directory. OpenShift Container Platform can sync those LDAP records with internal OpenShift Container Platform records, enabling you to manage your groups in one place. OpenShift Container Platform currently supports group sync with LDAP servers using three common schemas for defining group membership: RFC 2307, Active Directory, and augmented Active Directory. For additional information, refer to “Syncing Groups with LDAP” in the OpenShift Installation and Configuration guide:* [*https://docs.openshift.com/container-platform/3.3/install\_config/syncing\_groups\_with\_ldap.html*](https://docs.openshift.com/container-platform/3.3/install_config/syncing_groups_with_ldap.html)*>* |

* + - 1. Control Enhancement IA-2 (1)

The information system implements multifactor authentication for network access to privileged accounts.

|  |  |
| --- | --- |
| IA-2 (1) | Control Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| IA-2 (1) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for implementing multifactor authentication. Microsoft’s AAD and MFA solutions may be used for this purpose. A successful control response will need to address all user types and the means by which multifactor authentication is enforced for each.*>  *<OpenShift provides a pluggable authentication architecture that can utilize 3rd party authentication schemes that include multi-factor authentication. The authentication subsystem in OpenShift relies on OAuth 2.0 and any system that can interact with the OAuth token service over HTTPS can receive authentication tokens. Typically this is implemented using OpenShift’s provided RequestHeaderIdentityProvider as described in Section 12.3.8, “Request Header” of the OpenShift v3.3 Installation and Configuration Guide:*  [*https://docs.openshift.com/container-platform/3.3/install\_config/configuring\_authentication.html#RequestHeaderIdentityProvider*](https://docs.openshift.com/container-platform/3.3/install_config/configuring_authentication.html#RequestHeaderIdentityProvider) *>* |

* + - 1. Control Enhancement IA-2 (2)

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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| IA-2 (2) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for implementing multifactor authentication. Microsoft’s AAD and MFA solutions may be used for this purpose. A successful control response will need to address all user types and the means by which multifactor authentication is enforced for each.*>  *<OpenShift provides a pluggable authentication architecture that can utilize 3rd party authentication schemes that include multi-factor authentication. The authentication subsystem in OpenShift relies on OAuth 2.0 and any system that can interact with the OAuth token service over HTTPS can receive authentication tokens. Typically this is implemented using OpenShift’s provided RequestHeaderIdentityProvider as described in Section 12.3.8, “Request Header” of the OpenShift v3.3 Installation and Configuration Guide:*  [*https://docs.openshift.com/container-platform/3.3/install\_config/configuring\_authentication.html#RequestHeaderIdentityProvider*](https://docs.openshift.com/container-platform/3.3/install_config/configuring_authentication.html#RequestHeaderIdentityProvider) *>* |

* + - 1. Control Enhancement IA-2 (3)

The information system implements multifactor authentication for local access to privileged accounts.

| IA-2 (3) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: N/A | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| IA-2 (3) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*This control is not applicable for customers. Customers do not have local access to Microsoft Azure or OpenShift.*> |

* + - 1. Control Enhancement IA-2 (5)

The organization requires individuals to be authenticated with an individual authenticator when a group authenticator is employed.

| IA-2 (5) | Control Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| IA-2 (5) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  This is default, non-configurable behavior of the OpenShift Container Platform. All users, remote or local, administrative or non-privileged, first authenticate via an individual authenticator. Once individually authenticated, group access/privileges will be granted (if any). |

* + - 1. Control Enhancement IA-2 (8)

The information system implements replay-resistant authentication mechanisms for network access to privileged accounts.

| IA-2 (8) | Control Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| IA-2 (8) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for implementing replay-resistant authentication for access to privileged accounts. Microsoft’s AAD and MFA solutions may be used for this purpose. A successful control response will need to address all user types and the means by which replay-resistant authentication is required for each.*>  *<OpenShift can authenticate users against Microsoft Active Directory. It is recommended to use Active Directory if possible.>* |

* + - 1. Control Enhancement IA-2 (11)

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 [*Assignment: organization-defined strength of mechanism requirements*].

| IA-2 (11) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter IA-2(11): <*Customer defined strength of mechanism requirements*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| IA-2 (11) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for implementing multifactor authentication. Microsoft’s AAD and MFA solutions may be used for this purpose. A successful control response will need to address all user types and the means by which multifactor authentication is enforced for each, as well as the strength of mechanism required by the MFA solution.*> |

* + - 1. Control Enhancement IA-2 (12)

The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials.

**IA-2 (12) Additional FedRAMP Requirements and Guidance:** Include Common Access Card (CAC), i.e. the DoD technical implementation of PIV/FIPS 201/HSPD-12.

| IA-2 (12) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: N/A | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| IA-2 (12) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility:**  <*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*](https://www.microsoft.com/en-us/TrustCenter/Security/Identity)*.*> |

* + 1. Device Identification and Authentication (IA-3)

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*> | |
| Parameter IA-3-1: <*Customer defined virtual machines*> | |
| Parameter IA-3-2: <*Customer defined non-local connection*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| IA-3 What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for ensuring that customer-owned virtual machines are properly authenticated prior to establishing a connection to the rest of the customer system. A successful control response will need to address the virtual machines or types of virtual machines in use and the mechanism by which each is authenticated.*>  <OpenShift nodes can be configured with x509/PKI certificates, which will provide identity of the machines.> |

* + 1. Identifier Management (IA-4)

The organization manages information system identifiers for users and devices by:

1. Receiving authorization from [*Assignment: organization-defined personnel or roles*] to assign an individual, group, role, or device identifier;
2. Selecting an identifier that identifies an individual, group, role, or device;
3. Assigning the identifier to the intended individual, group, role, or device;
4. Preventing reuse of identifiers for [*FedRAMP Assignment: at least two years*]; and
5. Disabling the identifier after [*FedRMAP Assignment: ninety days for user identifiers; see additional requirements and guidance*]

**IA-4e Additional FedRAMP Requirements and Guidance: Requirement:** The service provider defines time period of inactivity for device identifiers.

| IA-4 | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter IA-4(a): <*Customer defined personnel or roles*> | |
| Parameter IA-4(d): <*FedRAMP requirement: at least two years*> | |
| Parameter IA-4(e): <*FedRAMP requirement: ninety days for user identifiers*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| IA-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for authorizing the assignment of identifiers. A successful control response will need to address the types of identifiers in use and the roles or personnel responsible for authorizing each type.*> |
| Part b | **Customer Responsibility**  <*The customer will be responsible for selecting identifiers. Microsoft’s AAD solution may be used for this purpose. A successful control response will need to address all identifier types and the means by which uniqueness of identifier is assured.*> |
| Part c | **Customer Responsibility**  <*The customer will be responsible for assigning identifiers. Microsoft’s AAD solution may be used for this purpose. A successful control response will need to address communication of the assigned identifier to individuals, groups, roles, or devices.*> |
| Part d | **Customer Responsibility**  <*The customer will be responsible for preventing the reuse of identifiers for the required timeframe. Microsoft’s AAD solution may be used for this purpose. Each account created within AAD is assigned a unique identifier (different from username, device name, etc.) which is never reused. A successful control response will need to address the types of identifiers in use and the means by which reuse is prevented.*> |
| Part e | **Customer Responsibility**  <*The customer will be responsible for disabling user identifiers after ninety days of inactivity, and other identifier types after customer-defined periods of inactivity. Microsoft’s AAD solution may be used for this purpose. A successful control response will need to address all identifier types and the means by which disabling takes place.*> |

* + - 1. Control Enhancement IA-4 (4)

The organization manages individual identifiers by uniquely identifying each individual as [*FedRAMP* *Assignment:* contractors; foreign nationals].

| IA-4 (4) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter IA-4(4): <*FedRAMP requirement: 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| IA-4 (4) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for including contractor or foreign national status as part of individual identifiers. Microsoft’s AAD solution may be used for this purpose. A successful control response will need to address how contractors and foreign nationals are identified by the customer and how that information is incorporated into the individual identifier.*> |

* + 1. Authenticator Management (IA-5)

The organization manages information system authenticators by:

1. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;
2. Establishing initial authenticator content for authenticators defined by the organization;
3. Ensuring that authenticators have sufficient strength of mechanism for their intended use;
4. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;
5. Changing default content of authenticators prior to information system installation;
6. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;
7. Changing/refreshing authenticators [*FedRAMP* *Assignment: to include 60 days for passwords*].
8. Protecting authenticator content from unauthorized disclosure and modification;
9. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and
10. Changing authenticators for group/role accounts when membership to those accounts changes.

| IA-5 | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter IA-5(g): <*FedRAMP requirement: 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| IA-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for verifying the identity of an individual, group, role, or device as part of authenticator distribution. A successful control response will need to address all account types in use and the means of verification for each (for example, verifying an individual’s identity with a government-issued identification card).*> |
| Part b | **Customer Responsibility**  <*The customer will be responsible for establishing initial authenticator content, such as initial passwords. Microsoft’s AAD solution may be used for this purpose. A successful control response will need to address all authenticator types and the means by which initial content is established for each.*> |
| Part c | **Customer Responsibility**  <*The customer will be responsible for enforcing strength requirements for authenticators. Microsoft’s AAD solution may be used for this purpose. A successful control response will need to address all authenticator types and the means by which strength of mechanism requirements are met for each.*> |
| Part d | **Customer Responsibility**  <*The customer will be responsible for establishing procedures for authenticator distribution, redistribution, and revocation. Microsoft’s AAD solution may be used for this purpose. A successful control response will need to address all authenticator types and scenarios, and the procedures established for each.*> |
| Part e | **Customer Responsibility**  <*The customer will be responsible for changing default authenticator content, such as default passwords for customer-installed software. A successful control response will address all situations within the customer application where a default authenticator may occur and the process by which changing the default content is enforced.*> |
| Part f | **Customer Responsibility**  <*The customer will be responsible for setting minimum and maximum lifetime restrictions and reuse conditions for authenticators. Microsoft’s AAD solution may be used for this purpose. A successful control response will need to address all authenticator types and the lifetime restrictions and reuse conditions for each.*> |
| Part g | **Customer Responsibility**  <*The customer will be responsible for refreshing authenticators at a regular cadence, to include every 60 days for passwords. Microsoft’s AAD solution may be used for this purpose. A successful control response will need to address all authenticator types, the refresh cadence for each, and the mechanism by which this cadence is enforced.*> |
| Part h | **Customer Responsibility**  <*The customer will be responsible for protecting authenticator content from unauthorized disclosure or modification. Microsoft’s AAD solution may be used for this purpose. A successful control response will need to address all authenticator types and the means used to protect each, as well as end user training to ensure that users do not disclose authenticators to unauthorized personnel.*> |
| Part i | **Customer Responsibility**  <*The customer will be responsible for implementing specific security safeguards to protect authenticators. Microsoft’s AAD solution may be used for this purpose. A successful control response will need to address all authenticator types and the means used to protect each, as well as end user training to ensure that users do not disclose authenticators to unauthorized personnel.*> |
| Part j | **Customer Responsibility**  <*The customer will be responsible for changing authenticators for group or role accounts when membership to those groups or roles changes. Microsoft’s AAD solution may be used for this purpose. A successful control response will need to discuss how group/role membership change is detected and reported, the personnel or roles responsible for changing the affected authenticators, and the process or mechanism used to perform the change.*> |

* + - 1. Control Enhancement IA-5 (1)

The information system, for password-based authentication:

1. Enforces minimum password complexity of [*FedRAMP* *Assignment:* [*case sensitive, minimum of twelve characters, and at least one each of upper-case letters, lower-case letters, numbers, and special characters*];
2. Enforces at least the following number of changed characters when new passwords are created: [*FedRAMP* *Assignment: at least one*];
3. Stores and transmits only cryptographically-protected passwords;
4. Enforces password minimum and maximum lifetime restrictions of [*FedRAMP* *Assignment: one day minimum, sixty day maximum*];
5. Prohibits password reuse for [*FedRAMP* *Assignment: twenty-four*] generations; and
6. Allows the use of a temporary password for system logons with an immediate change to a permanent password.

| IA-5 (1) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter IA-5(1)(a): <*FedRAMP requirement: [case sensitive, minimum of twelve characters, and at least one each of upper-case letters, lower-case letters, numbers, and special characters]*> | |
| Parameter IA-5(1)(b): <*FedRAMP requirement: at least one*> | |
| Parameter IA-5(1)(d): <*FedRAMP requirement: one day minimum, sixty day maximum*> | |
| Parameter IA-5(1)(e): <*FedRAMP requirement: twenty-four*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| IA-5 (1) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for enforcing the required password complexity. Microsoft’s AAD solution may be used for this purpose. A successful control response will need to address the mechanism used to enforce complexity.*> |
| Part b | **Customer Responsibility**  <*The customer will be responsible for enforcing the requirement to change at least one character when changing passwords. Microsoft’s AAD solution may be used for this purpose. A successful control response will need to address the mechanism used to enforce the required change.*> |
| Part c | **Customer Responsibility**  <*The customer will be responsible for storing and transmitting cryptographically-protected passwords. Microsoft’s AAD solution may be used for this purpose. Passwords stored by AAD are automatically hashed as part of AAD functionality. A successful control response will need to address the mechanism used to enforce cryptographic protection of passwords.*> |
| Part d | **Customer Responsibility**  <*The customer will be responsible for enforcing the required minimum and maximum lifetime restrictions. Microsoft’s AAD solution may be used for this purpose. A successful control response will need to address the mechanism used to enforce lifetime restrictions.*> |
| Part e | **Customer Responsibility**  <*The customer will be responsible for enforcing the required number of generations before password reuse. Microsoft’s AAD solution may be used for this purpose. A successful control response will need to address the mechanism used to enforce the reuse requirement.*> |
| Part f | **Customer Responsibility**  <*The customer will be responsible for enforcing the requirement to change initial/temporary passwords upon first login. Microsoft’s AAD solution may be used for this purpose. A successful control response will need to address the mechanism used to enforce the initial password change requirement.*> |

* + - 1. Control Enhancement IA-5 (2)

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 Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| IA-5 (2) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for validating certificates used within the customer application. Active Directory Certificate Services may be used for this purpose; for information, see the following TechNet article:* [*https://technet.microsoft.com/en-us/windowsserver/dd448615.aspx*](https://www.microsoft.com/en-us/trustcenter/security/auditingandlogging)*. A successful control response will need to address the mechanism used to validate certificates.*> |
| Part b | **Customer Responsibility**  <*The customer will be responsible for the enforcement of authorized access to private keys associated with certificates used within the customer application. Active Directory Certificate Services may be used for this purpose; for information, see the following TechNet article:* [*https://technet.microsoft.com/en-us/windowsserver/dd448615.aspx*](https://www.microsoft.com/en-us/TrustCenter/Security/Identity)*. A successful control response will need to address the mechanism used to restrict access to private keys.*> |
| Part c | **Customer Responsibility**  <*The customer will be responsible for mapping the identity authenticated by a certificate to the account of the individual or group associated with that identity. Active Directory Certificate Services may be used for this purpose; for information, see the following TechNet article:* [*https://technet.microsoft.com/en-us/windowsserver/dd448615.aspx*](https://technet.microsoft.com/en-us/windowsserver/dd448615.aspx)*. A successful control response will need to address the mechanism used to map identities between certificates and accounts.*> |
| Part d | **Customer Responsibility**  <*The customer will be responsible for implementing a local (i.e. within their subscription) cache of revocation data. Active Directory Certificate Services may be used for this purpose; for information, see the following TechNet article:* [*https://technet.microsoft.com/en-us/windowsserver/dd448615.aspx*](http://msdn.microsoft.com/en-us/library/azure/dn715779.aspx)*. A successful control response will need to address the mechanism used to establish and populate the revocation data.*> |

* + - 1. Control Enhancement IA-5 (3)

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 Enhancement Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter IA-5(3)-1: <*FedRAMP requirement: all hardware/biometric (multifactor) authenticators*> | |
| Parameter IA-5(3)-2: <*FedRAMP requirement: 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| IA-5 (3) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for distributing multifactor authenticators in person with proper authorizations in place. A successful control response will need to discuss the multifactor authenticators in use, the personnel or roles serving as the registration authority, and the personnel or roles providing authorization for distribution of the authenticators.*> |

* + - 1. Control Enhancement IA-5 (4)

The organization employs automated tools to determine if password authenticators are sufficiently strong to satisfy [*Assignment: organization-defined requirements*].

**IA-5(4) Additional FedRAMP Requirements and Guidance:** Guidance: If automated mechanisms which enforce password authenticator strength at creation are not used, automated mechanisms must be used to audit strength of created password authenticators

| IA-5 (4) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter IA-5(4): <*Customer defined requirements*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| IA-5 (4) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for employing automated tools to ensure that password authenticators meet strength requirements. Microsoft’s AAD solution may be used for this purpose. A successful control response will need to address the automated mechanism used to enforce password strength requirements.*> |

* + - 1. Control Enhancement IA-5 (6)

The organization protects authenticators commensurate with the security category of the information to which use of the authenticator permits access.

| IA-5 (6) | Control Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| IA-5 (6) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for protecting authenticators. Microsoft’s AAD solution may be used for this purpose. A successful control response will need to address the mechanisms, processes, or tools used to protect authenticators.*> |

* + - 1. Control Enhancement IA-5 (7)

The organization ensures that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys.

| IA-5 (7) | Control Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| IA-5 (7) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for ensuring that unencrypted static authenticators are not embedded or stored. A successful control response will need to address both policy requirements and technical enforcement mechanisms.*> |

* + - 1. Control Enhancement IA-5 (11)

The information system, for hardware token-based authentication, employs mechanisms that satisfy [*Assignment: organization-defined token quality requirements*].

| IA-5 (11) | Control Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| IA-5 (11) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for employing automated tools to ensure that hardware tokens meet customer-defined token quality requirements. A successful control response will need to discuss the quality requirements in place, the rational for those requirements, and the means by which hardware tokens are shown to meet those requirements.*> |

* + 1. Authenticator Feedback (IA-6)

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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| IA-6 What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for obscuring authentication feedback information during the authentication process for any customer applications. A successful control response will need to address the various authentication scenarios that might arise and the mechanism used to obscure feedback during each.*> |

* + 1. Cryptographic Module Authentication (IA-7)

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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| IA-7 What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  *<Administrative access to OpenShift nodes is perfomed over SSH. To limit SSH ciphers to those algorithms which are FIPS-approved, update the following line in /etc/ssh/sshd\_config:  Ciphers aes128-ctr,aes192-ctr,aes256-ctr>*  *<The OpenShift Console, which is the web interface to the system, converts incoming authentication requests to HTTPS automatically.>* |

* + 1. Identification and Authentication (Non-Organizational Users) (IA-8)

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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| IA-8 What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for identifying and authenticating non-organizational users accessing the customer application. A successful control response will need to address how non-organizational users are defined and the process by which identification and authentication takes place, including any differences from identification and authentication for organizational users.*> |

* + - 1. Control Enhancement IA-8 (1)

The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials from other federal agencies.

| IA-8 (1) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: N/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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| IA-8 (1) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility:**  <*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*](http://usgcb.nist.gov/usgcb_faq.html)*.*> |

* + - 1. Control Enhancement IA-8 (2)

The information system accepts only FICAM-approved third-party credentials.

| IA-8 (2) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: N/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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| IA-8 (2) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility:**  <*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). For more information about ADFS, see the following TechNet article:* [*https://technet.microsoft.com/en-us/magazine/dn250023.aspx*](https://technet.microsoft.com/en-us/windowsserver/dd448615.aspx)*.*> |

* + - 1. Control Enhancement IA-8 (3)

The organization employs only FICAM-approved information system components in [*Assignment: organization-defined information systems*] to accept third-party credentials.

| IA-8 (3) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: N/A | |
| Parameter IA-8(3): N/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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| IA-8 (3) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility:**  <*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). For more information about ADFS, see the following TechNet article:* [*https://technet.microsoft.com/en-us/magazine/dn250023.aspx*](https://azure.microsoft.com/en-us/documentation/articles/active-directory-hybrid-identity-design-considerations-overview/)*.*> |

* + - 1. Control Enhancement IA-8 (4)

The information system conforms to FICAM-issued profiles.

| IA-8 (4) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: N/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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| IA-8 (4) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility:**  <*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). For more information about ADFS, see the following TechNet article:* [*https://technet.microsoft.com/en-us/magazine/dn250023.aspx*](https://technet.microsoft.com/en-us/magazine/dn250023.aspx)*.*> |

* 1. Incident Response (IR)
     1. Incident Response Policy and Procedures (IR-1)

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 every 3 years*]; and
   2. Incident response procedures [*FedRAMP Assignment: at least annually*].

| IR-1 | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter IR-1(a): <*Customer-defined personnel or roles*> | |
| Parameter IR-1(b)(1): <*FedRAMP requirement: at least every 3 years*> | |
| Parameter IR-1(b)(2): <*FedRAMP requirement: 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) | |

| IR-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for developing, documenting, and disseminating Incident Response policy and procedures. A successful control response will need to address the content of the policy (which must include purpose, scope, roles, responsibilities, management commitment, coordination, and compliance) and procedures (which must facilitate the implementation of the policies and associated controls).*> |
| Part b | **Customer Responsibility**  <*The customer will be responsible for reviewing and updating the Incident Response policy every 3 years, and procedures annually. A successful control response will need to address the review and update process, including the role(s) responsible for initiating the review process, updating the policy and procedures, and providing approval of the updates.*> |

* + 1. Incident Response Training (IR-2)

The organization provides incident response training to information system users consistent with assigned roles and responsibilities:

1. Within [*Assignment: organization-defined time period*] 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): <*Customer defined time period*> | |
| Parameter IR-2(c): <*FedRAMP requirement: at least annually*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| IR-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  *<The customer will be responsible for initial training related to contingency plan activities. This training will need to include consideration for all aspects of incident response that are the responsibility of the customer. A successful control response will need to outline the scope and contents of the training, the audience for the training, and the means by which training attendance is tracked and enforced.>* |
| Part b | **Customer Responsibility**  *<The customer will be responsible for providing retraining related to contingency plan activities as required by information system changes. A successful control response will need to address identification of changes that require retraining as well as notification to relevant parties that retraining is required and tracking/enforcement of attendance.>* |
| Part c | **Customer Responsibility**  *<The customer will be responsible for refresher training related to contingency plan activities at the required frequency. A successful control response will need to address the means by which refresher training attendance is tracked and enforced.>* |

* + 1. Incident Response Testing (IR-3)

The organization tests the incident response capability for the information system [*FedRAMP Assignment: at least annually*] using [*FedRAMP Assignment: See Additional FedRAMP Requirements and Guidance*] to determine the incident response effectiveness and documents the results.

**Additional FedRAMP Requirements and Guidance:** Requirement: 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 Authorizing Official (AO) annually. Test plans are approved and accepted by the AO prior to the test commencing.

|  |  |
| --- | --- |
| IR-3 | Control Summary Information |
| Responsible Role: <*Customer defined*> | |
| Parameter IR-3-1: <*FedRAMP requirement: at least annually*> | |
| Parameter IR-3-2: <*FedRAMP requirement: tests and exercises in accordance with NIST Special Publication 800-61*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| IR-3 What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  *<The customer will be responsible for testing of incident response plans at the required frequency. A successful control response will need to address the scenarios and exercises chosen for the test, as well as the process for documenting and reviewing test results. Test plans will need to be approved by the Authorizing Official prior to the test commencing.*  *NIST Special Publication 800-61, Rev. 2.,* Computer Security Incident Handling Guide*, provides guidance on the development and testing of incident response plans.>* |

* + - 1. Control Enhancement IR-3 (2)

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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | | | |

|  |
| --- |
| IR-3 (2) What is the solution and how is it implemented? |
| **Customer Responsibility**  <*The customer will be responsible for coordinating testing of the incident response plan with related plans (such as business continuity plans, contingency plans, etc.). A successful control response will need to address ensuring that any test results relevant to related plans are communicated so that corrective actions may be taken as needed.*> |

* + 1. Incident Handling (IR-4)

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.

**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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| IR-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for developing incident response plans and testing that includes consideration for any controls that are the responsibility of the customer relating to shared touch points included in the customer’s authorization boundary and any customer applications leveraging the provider’s infrastructure. Incident handling for customer applications is the responsibility of the customer unless an incident is caused by Microsoft or the result of Microsoft action. A successful control response will need to address the required steps in incident response (preparation, detection and analysis, containment, eradication, and recovery), including identifying roles or individuals responsible for each step.*  *Microsoft Azure has created the article “Managing and responding to security alerts in Azure Security Center”, which customers may use in the development of incident response plans:* [*https://azure.microsoft.com/en-us/documentation/articles/security-center-managing-and-responding-alerts/*](https://technet.microsoft.com/en-us/windowsserver/dd448615.aspx)*.*> |
| Part b | **Customer Responsibility**  <*The customer will be responsible for incident handling activities with contingency plan activities. A successful control response will need to address communication and prioritization in the case of conflicts (for example, if incident analysis and containment causes delays in service restoration).*> |
| Part c | **Customer Responsibility**  <*The customer will be responsible for updating incident response plans, procedures, training and testing based on lessons learned from incident handling activities. A successful control response will need to address the personnel or roles responsible for gathering and reviewing lessons learned, updating plans, procedures, training, and testing, and reviewing and signing off on changes.*> |

* + - 1. Control Enhancement IR-4 (1)

The organization employs automated mechanisms to support the incident handling process.

| IR-4 (1) | Control Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| IR-4 (1) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for using automated mechanisms (such as ticketing systems and incident tracking/reporting systems) in support of customer incident handling activities. A successful control response will need to address the automated systems involved and their place within the overall incident handling process.*> |

* + 1. Incident Monitoring (IR-5)

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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| IR-5 What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for tracking and documenting information system security incidents. A successful control response will need to address the tools and processes used for documentation, and relate these tools and processes to the automated mechanisms used in IR-4(1).*> |

* + 1. Incident Reporting (IR-6)

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 requirement: US-CERT incident reporting timelines as specified in NIST SP 800-61 (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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| IR-6 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for requiring personnel to report suspected security incidents within the required timeframes. A successful control response will need to address examples of events that personnel should report, as well as tools, mechanisms, and processes used for reporting.*> |
| Part b | **Customer Responsibility**  <*The customer will be responsible for reporting security incident information according to the FedRAMP Incident Communications Procedure. In cases where customer security incidents may affect the security status of Microsoft Azure as a whole, the customer will be responsible for notifying Microsoft Azure as well. A successful control response will need to address the individuals or roles responsible for such notification.*> |

* + - 1. Control Enhancement IR-6 (1)

The organization employs automated mechanisms to assist in the reporting of security incidents**.**

| IR-6 (1) | Control Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| IR-6 (1) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for using automated mechanisms (such as ticketing systems and incident tracking/reporting systems) in support of the reporting of security incidents. A successful control response will need to address the automated systems involved and how they are used for reporting of incidents.*> |

* + 1. Incident Response Assistance (IR-7)

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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| IR-7 What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for providing incident response resources to their users. These resources may be, for example, web pages, helpdesk resources, or assistance groups. A successful control response will need to outline the resources available and discuss how users are notified of the existence of these resources.*> |

* + - 1. Control Enhancement IR-7 (1)

The organization employs automated mechanisms to increase the availability of incident response related information and support.

| IR-7 (1) | Control Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| IR-7 (1) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for using automated mechanisms (such as websites or email distribution lists) to increase the availability of incident response support resources. A successful control response will need to discuss the mechanisms used and the information and support resources provided via each mechanism.*> |

* + - 1. Control Enhancement IR-7 (2)

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 Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| IR-7 (2) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for establishing relationships between its incident response capability and external providers. In particular, 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. Additionally, the customer is responsible to designate US-CERT as a notification contact. A successful control response will need to address these requirements as well as relationships with any other relevant external providers of information system protection capability.*> |
| Part b | **Customer Responsibility**  <*The customer will be responsible for identifying incident response team members to Microsoft Azure and any other external providers. A successful control response will need to discuss the means by which this identification is communicated.*> |

* + 1. Incident Response Plan (IR-8)

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): <*Customer defined incident response personnel; FedRAMP requirement: includes designated FedRAMP personnel*> | |
| Parameter IR-8(c): <*FedRAMP requirement: at least annually*> | |
| Parameter IR-8(e): <*Customer defined incident response personnel; FedRAMP requirement: 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| IR-8 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for developing an incident response plan that includes consideration for any controls that are the responsibility of the customer relating to shared touch points included in the customer’s authorization boundary and any customer applications leveraging the provider’s infrastructure. A successful control response will need to address how the plan meets each of the specified requirements, and the individuals or roles responsible for ensuring that the requirements are met.*> |
| Part b | **Customer Responsibility**  <*The customer will be responsible for distributing the incident response plan to identified internal and FedRAMP personnel. A successful control response will need to address the criteria for inclusion in the distribution list.*> |
| Part c | **Customer Responsibility**  <*The customer will be responsible for reviewing the incident response plan at the required frequency. A successful control response will need to address how the review process is initiated and the roles or individuals responsible for performing the review.*> |
| Part d | **Customer Responsibility**  <*The customer will be responsible for updating the incident response plan as appropriate. A successful control response will need to address the criteria for requiring an update to the incident response plan, the individuals or roles responsible for updating the plan, and the process for approval of updates.*> |
| Part e | **Customer Responsibility**  <*The customer will be responsible for communicating changes made to the incident response plan to the list of internal and FedRAMP personnel identified in part (b).*> |
| Part f | **Customer Responsibility**  <*The customer will be responsible for protecting the incident response plan from unauthorized disclosure or modification. A successful control response will need to address policy, procedural, and technical safeguards that are in place to protect the incident response plan.*> |

* + 1. Information Spillage Response (IR-9)

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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | | | |

|  |  |
| --- | --- |
| IR-9 What is the solution and how is it implemented? | |
| Part a | **Customer Responsibility**  <*The customer will be responsible for identifying the specific information involved in an information spill. A successful control response will need to address how spills are detected and the tools or processes used to identify the specific information involved.*> |
| Part b | **Customer Responsibility**  <*The customer will be responsible for alerting designated personnel using a non-contaminated method of communication. A successful control response will need to discuss how the personnel are designated and notified.*> |
| Part c | **Customer Responsibility**  <*The customer will be responsible for isolating the contaminated system or component. This may involve, for example, disabling connections to the component or shutting it down. A successful control response will need to address the types of components that could potentially be contaminated and the mechanism for isolating each type.*> |
| Part d | **Customer Responsibility**  <*The customer will be responsible for eradicating the spilled information from the contaminated system or component. A successful control response will need to address the means by which eradication is carried out and confirmed.*> |
| Part e | **Customer Responsibility**  <*The customer will be responsible for identifying other systems or components that may have been contaminated subsequent to the initial spill. A successful control response will need to outline the investigative process used to make this determination.*> |
| Part f | **Customer Responsibility**  <*The customer will be responsible for identifying and performing any additional required actions to resolve information spills. A successful control response will need to address how those actions are identified and the roles or individuals responsible for identifying and performing the actions.*> |

* + - 1. Control Enhancement IR-9 (1)

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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | | | |

|  |
| --- |
| IR-9 (1) What is the solution and how is it implemented? |
| **Customer Responsibility**  <*The customer will be responsible for identifying personnel or roles with responsibility for responding to information spills. This may be all members of the incident response team, specific members with specialized knowledge, or individuals or teams completely distinct from the incident response team. A successful control response will need to address the rationale for the selection.*> |

* + - 1. Control Enhancement IR-9 (2)

The organization provides information spillage response training [*Assignment: organization defined frequency*].

|  |  |
| --- | --- |
| IR-9 (2) | Control Summary Information |
| Responsible Role: <*Customer defined*> | |
| Parameter IR-9(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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | | | |

|  |
| --- |
| IR-9 (2) What is the solution and how is it implemented? |
| **Customer Responsibility**  <*The customer will be responsible for providing information spillage response training on a regular basis. This may be incorporated into overall incident response training or may be a separate training course or module. A successful control response will need to outline the contents of the information spillage response training and address the frequency at which training is provided.*> |

* + - 1. Control Enhancement IR-9 (3)

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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | | | |

|  |
| --- |
| IR-9 (3) What is the solution and how is it implemented? |
| **Customer Responsibility**  <*The customer will be responsible for defining and implementing procedures to allow personnel affected by information spills to continue carrying out assigned tasks during the information spill response process. A successful control response will need to address, for example, alternate means of connection to affected systems and changes to processes required to employ those alternate means.*> |

* + - 1. Control Enhancement IR-9 (4)

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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | | | |

|  |
| --- |
| IR-9 (4) What is the solution and how is it implemented? |
| **Customer Responsibility**  <*The customer will be responsible for defining and employing additional safeguards for personnel exposed to information they were not authorized to access. These may include, for example, additional training, non-disclosure agreements, etc. A successful control response will need to address the nature of these safeguards and whether they are employed proactively (prior to information spillage incidents) or reactively (following information spillage incidents).*> |

* 1. Maintenance (MA)
     1. System Maintenance Policy and Procedures (MA-1)

The organization:

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

| MA-1 | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter MA-1(a): <*Customer-defined personnel or roles*> | |
| Parameter MA-1(b)(1): <*FedRAMP requirement: at least every 3 years*> | |
| Parameter MA-1(b)(2): <*FedRAMP requirement: 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) | |

| MA-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for developing, documenting, and disseminating System Maintenance policy and procedures. A successful control response will need to address the content of the policy (which must include purpose, scope, roles, responsibilities, management commitment, coordination, and compliance) and procedures (which must facilitate the implementation of the policies and associated controls).*> |
| Part b | **Customer Responsibility**  <*The customer will be responsible for reviewing and updating the System Maintenance policy every 3 years, and procedures annually. A successful control response will need to address the review and update process, including the role(s) responsible for initiating the review process, updating the policy and procedures, and providing approval of the updates.*> |

* + 1. Controlled Maintenance (MA-2)

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: Microsoft Azure | |
| Parameter MA-2(c): Datacenter Management, Property asset owners | |
| Parameter MA-2(f): (i) the date and time of maintenance; (ii) name of the individual performing the maintenance; (iii) name of escort, if necessary; (iv) a description of the maintenance performed; and (v) a list of equipment removed or replaced (including identification numbers, if applicable). | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| MA-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.3.2. |
| Part b | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.3.2. |
| Part c | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.3.2. |
| Part d | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.3.2. |
| Part e | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.3.2. |
| Part f | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.3.2. |

* + 1. Maintenance Tools (MA-3)

The organization approves, controls, and monitors information system maintenance tools.

| MA-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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| MA-3 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.3.3. |

* + - 1. Control Enhancement MA-3 (1)

The organization inspects the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.

| MA-3 (1) | Control Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| MA-3 (1) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.3.3.1. |

* + - 1. Control Enhancement MA-3 (2)

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 Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| MA-3 (2) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.3.3.2. |

* + - 1. Control Enhancement MA-3 (3)

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 authorizing removal of the equipment from the facility.

| MA-3 (3) | Control Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| MA-3 (3) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.3.3.3. |

* + 1. Remote Maintenance (MA-4)

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*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| MA-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  *<The customer will be responsible for approving and monitoring non-local maintenance and diagnostic activities. Because of the nature of a cloud system, all maintenance and diagnostic activities will be considered non-local. Therefore, this control can largely be addressed by reference to access control authorizations (see AC-2) and the auditing and monitoring discussions in the AU family and SI-4. A successful control response will need to address the personnel or roles who are authorized to perform maintenance and diagnostic activities, and how those activities are tracked.>* |
| Part b | **Customer Responsibility**  *<The customer will be responsible for ensuring that non-local maintenance and diagnostic activities and tools are consistent with the customer’s policies. A successful control response will need to discuss ensuring that, for example, authorization, identification, and authentication policies are followed for all personnel and tools performing maintenance and diagnostic activities.>* |
| Part c | **Customer Responsibility**  *<The customer will be responsible for ensuring that strong authenticators are used to establish non-local maintenance and diagnostic sessions. A successful control response will need to discuss ensuring that authenticators are resistant to replay attacks and employ multifactor authentication.>* |
| Part d | **Customer Responsibility**  *<The customer will be responsible for maintaining records of non-local maintenance and diagnostic activities. A successful control response will need to address the types of activities for which records are kept as well as the contents of those records.>* |
| Part e | **Customer Responsibility**  *<The customer will be responsible for terminating the session and network connections when non-local maintenance and diagnostic activities are completed. A successful control response will need to address monitoring and enforcement of the disconnection requirement.>* |

* + - 1. Control Enhancement MA-4 (2)

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 Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| MA-4 (2) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  *<The customer will be responsible for documenting the policies and procedures for the establishment and use of non-local maintenance and diagnostic connections. A successful control response will need to address when non-local maintenance and diagnostic connections are allowed, what personnel are authorized to establish and use them, and under what circumstances connections must be terminated.>* |

* + 1. Maintenance Personnel (MA-5)

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: 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| MA-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.3.5. |
| Part b | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.3.5. |
| Part c | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.3.5. |

* + - 1. Control Enhancement MA-5 (1)

The organization:

1. Implements procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, that include the following requirements:
   1. Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the information system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified;
   2. Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the information system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured; and
2. Develops and implements alternate security safeguards in the event an information system component cannot be sanitized, removed, or disconnected from the system

**MA-5 (1) Additional FedRAMP Requirements and Guidance:** Requirement: Only MA-5 (1)(a)(1) is required by FedRAMP Moderate Baseline

| MA-5 (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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| MA-5 (1) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.3.5.1. |
| Part b | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.3.5.1. |

* + 1. Timely Maintenance (MA-6)

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: Microsoft Azure | |
| Parameter MA-6-1: Critical components list via CMMS | |
| Parameter MA-6-2: Spare part/vendor agreements are acquired as needed to support the replacement SLAs. | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| MA-6 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.3.6. |

* 1. Media Protection (MP)
     1. Media Protection Policy and Procedures (MP-1)

The organization:

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

| MP-1 | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter MP-1(a): <*Customer-defined personnel or roles*> | |
| Parameter MP-1(b)(1): <*FedRAMP requirement: at least every 3 years*> | |
| Parameter MP-1(b)(2): <*FedRAMP requirement: 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) | |

| MP-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for developing, documenting, and disseminating Media Protection policy and procedures. A successful control response will need to address the content of the policy (which must include purpose, scope, roles, responsibilities, management commitment, coordination, and compliance) and procedures (which must facilitate the implementation of the policies and associated controls).*> |
| Part b | **Customer Responsibility**  <*The customer will be responsible for reviewing and updating the Media Protection policy every 3 years, and procedures annually. A successful control response will need to address the review and update process, including the role(s) responsible for initiating the review process, updating the policy and procedures, and providing approval of the updates.*> |

* + 1. Media Access (MP-2)

The organization restricts access to [*Assignment: organization-defined types of digital and/or non-digital media*] to [*Assignment: organization-defined personnel or roles*].

| MP-2 | Control Summary Information |
| --- | --- |
| Responsible Role: Microsoft Azure | |
| Parameter MP-2-1: Server assets and magnetic backup tapes secured at Microsoft datacenters | |
| 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| MP-2 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.4.2. |

* + 1. Media Labeling (MP-3)

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* *FedRAMP Assignment: parameter not applicable*]

**MP-3(b) Additional FedRAMP Requirements and Guidance:** **Guidance:** Second parameter in MP-3(b) 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: N/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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| MP-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.4.3. |
| Part b | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.4.3. |

* + 1. Media Storage (MP-4)

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 by Microsoft 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| MP-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.4.4. |
| Part b | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.4.4. |

* + 1. Media Transport (MP-5)

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.

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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| MP-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.4.5. |
| Part b | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.4.5. |
| Part c | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.4.5. |
| Part d | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.4.5. |

* + - 1. Control Enhancement MP-5 (4)

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 Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| MP-5 (4) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.4.5.1. |

* + 1. Media Sanitization and Disposal (MP-6)

The organization:

1. Sanitizes [*Assignment: organization-defined information system media*] prior to disposal, release out of organizational control, or release for reuse using [*Assignment: organization-defined sanitization techniques and procedures*] in accordance with applicable federal and organizational standards and policies; and
2. Employs sanitization mechanisms with strength and integrity commensurate with the classification or classification of the information.

| MP-6 | Control Summary Information |
| --- | --- |
| Responsible Role: 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| MP-6 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.4.6. |
| Part b | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.4.6. |

* + - 1. Control Enhancement MP-6 (2)

The organization tests sanitization equipment and procedures [*FedRAMP Assignment: at least annually*] to verify that the intended sanitization is being achieved.

**MP-6(2) Additional FedRAMP Requirements and Guidance: Guidance:** Equipment and procedures may be tested or evaluated for effectiveness.

| MP-6 (2) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: Microsoft Azure | |
| Parameter MP-6(2): Annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| MP-6 (2) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.4.6.1. |

* + 1. Media Use (MP-7)

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 Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | | |

|  |
| --- |
| MP-7 What is the solution and how is it implemented? |
| **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.4.7. |

* + - 1. Control Enhancement MP-7 (1)

The organization prohibits the use of portable storage devices in organizational information systems when such devices have no identifiable owner.

|  |  |
| --- | --- |
| MP-7 (1) | Control Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

|  |
| --- |
| MP-7 (1) What is the solution and how is it implemented? |
| **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.4.7.1. |

* 1. Physical and Environmental Protection (PE)
     1. Physical and Environmental Protection Policy and Procedures (PE-1)

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 every 3 years*]; and
   2. Physical and environmental protection procedures [*FedRAMP Assignment: at least annually*].

| PE-1 | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter PE-1(a): <*Customer-defined personnel or roles*> | |
| Parameter PE-1(b)(1): <*FedRAMP requirement: at least every 3 years*> | |
| Parameter PE-1(b)(2): <*FedRAMP requirement: 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) | |

| PE-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for developing, documenting, and disseminating Physical and Environmental Protection policy and procedures. A successful control response will need to address the content of the policy (which must include purpose, scope, roles, responsibilities, management commitment, coordination, and compliance) and procedures (which must facilitate the implementation of the policies and associated controls).*> |
| Part b | **Customer Responsibility**  <*The customer will be responsible for reviewing and updating the Physical and Environmental Protection policy every 3 years, and procedures annually. A successful control response will need to address the review and update process, including the role(s) responsible for initiating the review process, updating the policy and procedures, and providing approval of the updates.*> |

* + 1. Physical Access Authorizations (PE-2)

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 annually*]; 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): Annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| PE-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.5.2. |
| Part b | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.5.2. |
| Part c | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.5.2. |
| Part d | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.5.2. |

* + 1. Physical Access Control (PE-3)

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 Enhancement 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, locks, and/or alarms | |
| Parameter PE-3(d): At all times while in the data center | |
| Parameter PE-3(f): Keys, temporary access badges, access badge readers, and similar devices; 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| PE-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.5.3. |
| Part b | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.5.2. |
| Part c | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.5.2. |
| Part d | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.5.2. |
| Part e | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.5.2. |
| Part f | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.5.2. |
| Part g | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.5.2. |

* + 1. Access Control for Transmission Medium (PE-4)

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 Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| PE-4 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.5.4. |

* + 1. Access Control for Output Devices (PE-5)

The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.

| PE-5 | Control Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| PE-5 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.5.5. |

* + 1. Monitoring Physical Access (PE-6)

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: Quarterly | |
| 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| PE-6 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.5.6. |
| Part b | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.5.6. |
| Part c | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.5.6. |

* + - 1. Control Enhancement PE-6 (1)

The organization monitors physical intrusion alarms and surveillance equipment.

| PE-6 (1) | Control Enhancement 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)  Hybrid (Service Provider and Customer)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| PE-6 (1) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.5.6.1. |

* + 1. Visitor Access Records (PE-8)

The organization:

1. Maintains visitor access records to the facility where the information system resides for [*FedRAMP Assignment: for a minimum of one 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| PE-8 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.5.7. |
| Part b | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.5.7. |

* + 1. Power Equipment and Cabling (PE-9)

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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| PE-9 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.5.8. |

* + 1. Emergency Shutoff (PE-10)

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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| PE-10 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.5.9. |
| Part b | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.5.9. |
| Part c | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.5.9. |

* + 1. Emergency Power (PE-11)

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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| PE-11 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.5.10. |

* + 1. Emergency Lighting (PE-12)

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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| PE-12 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.5.11. |

* + 1. Fire Protection (PE-13)

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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| PE-13 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.5.12. |

* + - 1. Control Enhancement PE-13 (2)

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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| PE-13 (2) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.5.12.1. |

* + - 1. Control Enhancement PE-13 (3)

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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| PE-13 (3) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.5.12.2. |

* + 1. Temperature and Humidity Controls (PE-14)

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
2. Monitors temperature and humidity levels [*FedRAMP Assignment: continuously*]

**PE-14(a) Additional FedRAMP Requirements and Guidance: Requirement:** The service provider measures temperature at server inlets and humidity levels by dew point.

| 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 ranges 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| PE-14 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.5.13. |
| Part b | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.5.13. |

* + - 1. Control Enhancement PE-14 (2)

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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

|  |
| --- |
| PE-14 (2) What is the solution and how is it implemented? |
| **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.5.13.1. |

* + 1. Water Damage Protection (PE-15)

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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| PE-15 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.5.14. |

* + 1. Delivery and Removal (PE-16)

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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| PE-16 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.5.15. |

* + 1. Alternate Work Site (PE-17)

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)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| PE-17 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.5.16. |
| Part b | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.5.16. |
| Part c | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.5.16. |

* 1. Planning (PL)
     1. Security Planning Policy and Procedures (PL-1)

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 every three years*]; and
   2. Security planning procedures [*FedRAMP Assignment: at least annually*].

| PL-1 | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter PL-1(a): <*Customer-defined personnel or roles*> | |
| Parameter PL-1(b)(1): <*FedRAMP requirement: at least every 3 years*> | |
| Parameter PL-1(b)(2): <*FedRAMP requirement: 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) | |

| PL-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for developing, documenting, and disseminating Security Planning policy and procedures. A successful control response will need to address the content of the policy (which must include purpose, scope, roles, responsibilities, management commitment, coordination, and compliance) and procedures (which must facilitate the implementation of the policies and associated controls).*> |
| Part b | **Customer Responsibility**  <*The customer will be responsible for reviewing and updating the Security Planning policy every 3 years, and procedures annually. A successful control response will need to address the review and update process, including the role(s) responsible for initiating the review process, updating the policy and procedures, and providing approval of the updates.*> |

* + 1. System Security Plan (PL-2)

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 requirement: at least annually*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| PL-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  *<The customer will be responsible for developing a system security plan (this document) in accordance with the above requirements. A successful control response will need to address each of the requirements and how this document meets them.*  *The customer may wish to consult NIST Special Publication 800-18, Revision 1,* Guide for Developing Security Plans for Federal Information Systems*, which contains guidance on security planning. Portions of this system security plan will discuss controls inherited from Microsoft Azure and will refer to the Microsoft Azure SSP. Government agencies who wish to review the Azure SSP may request it via the service trust portal:* [*https://www.microsoft.com/trustcenter/stp*](https://www.microsoft.com/en-us/TrustCenter/Security/Identity)*.>* |
| Part b | **Customer Responsibility**  *<The customer will be responsible for distributing the system security plan to relevant personnel and keeping those personnel informed of subsequent changes. A successful control response will need to address identifying personnel who should receive a copy of the system security plan, as well as ensuring all such personnel are notified appropriately.>* |
| Part c | **Customer Responsibility**  *<The customer will be responsible for reviewing the system security plan at the required frequency. A successful control response will need to address the initiation of the review process and the roles or individuals responsible for review.>* |
| Part d | **Customer Responsibility**  *<The customer will be responsible for updating the system security plan to address changes to the information system and its environment or any problems identified during implementation or security assessments. A successful control response will need to discuss the roles or individuals responsible for updating the plan, as well as the process for approval of any updates.>* |
| Part e | **Customer Responsibility**  *<The customer will be responsible for protecting the security plan from unauthorized disclosure or modification. A successful control response will need to address policy, procedural, and technical safeguards that are in place to protect the system security plan.>* |

* + - 1. Control Enhancement PL-2 (3)

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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

|  |
| --- |
| PL-2 (3) What is the solution and how is it implemented? |
| **Customer Responsibility**  *<The customer will be responsible for planning and coordinating security-related activities so as to reduce the impact on other organizational entities. These activities may include security assessments, audits, maintenance, patch management, and contingency plan testing. A successful control response will need to address the process by which other organizational entities are notified of and consulted regarding such activities.>* |

* + 1. Rules of Behavior (PL-4)

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: at least every three years*]; 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 requirement: at least every three years*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| PL-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  *<The customer will be responsible for defining, documenting, and distributing rules of behavior. A successful control response will need to outline the rules of behavior and discuss the process for making them available to users requiring access to the system.>* |
| Part b | **Customer Responsibility**  *<The customer will be responsible for obtaining signed acknowledgment of the rules of behavior from its users. A successful control response will need to address the process for withholding authorization until signatures are obtained.>* |
| Part c | **Customer Responsibility**  *<The customer will be responsible for reviewing and updating the rules of behavior at the required frequency. A successful control response will need to address the process for initiating review, as well as the individuals or roles responsible for carrying out the review, managing updates, and approving the final version.>* |
| Part d | **Customer Responsibility**  *<The customer will be responsible for obtaining signed acknowledgment of the updated rules of behavior. A successful control response will need to address the process for removing authorization if signatures are not obtained in a timely manner.>* |

* + - 1. Control Enhancement PL-4 (1)

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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | | |

|  |
| --- |
| PL-4 (1) What is the solution and how is it implemented? |
| **Customer Responsibility**  *<The customer will be responsible for incorporating explicit restrictions on the use of social media/networking sites and posting organizational information on public websites into the rules of behavior. A successful control response will need to outline the relevant portions of the rules of behavior.>* |

* + 1. Information Security Architecture (PL-8)

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*] to reflect updates in the enterprise architecture; and
3. 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): <*FedRAMP requirement: at least annually*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| PL-8 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  *<The customer will be responsible for developing their information security architecture. A successful control response will need to discuss the guiding principles used to protect confidentiality, integrity, and availability of system information and the dependencies on external services (such as Microsoft Azure). Additionally, a description of the information security architecture should be included in the introductory sections of this system security plan.*  *Microsoft Azure has created the page “Getting Started with Microsoft Azure Security”, which customers may use to guide them in developing the information security architecture:* [*https://azure.microsoft.com/en-us/documentation/articles/azure-security-getting-started/*](http://msdn.microsoft.com/en-us/library/azure/dn715779.aspx)*.>* |
| Part b | **Customer Responsibility**  *<The customer will be responsible for reviewing and updating the security architecture at the required frequency. A successful control response will need to address the process for initiating review, as well as the individuals or roles responsible for carrying out the review, managing updates, and approving the final version.>* |
| Part c | **Customer Responsibility**  *<The customer will be responsible for incorporating changes to the security architecture into this system security plan as well as related materials. A successful control response will need to address the process for aligning the contents of the system security plan with the information security architecture, including the individuals or roles responsible for that alignment.>* |

* 1. Personnel Security (PS)
     1. Personnel Security Policy and Procedures (PS-1)

The organization**:**

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

| PS-1 | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter PS-1(a): <*Customer-defined personnel or roles*> | |
| Parameter PS-1(b)(1): <*FedRAMP requirement: at least every 3 years*> | |
| Parameter PS-1(b)(2): <*FedRAMP requirement: 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 | **Customer Responsibility**  <*The customer will be responsible for developing, documenting, and disseminating Personnel Security policy and procedures. A successful control response will need to address the content of the policy (which must include purpose, scope, roles, responsibilities, management commitment, coordination, and compliance) and procedures (which must facilitate the implementation of the policies and associated controls).*> |
| Part b | **Customer Responsibility**  <*The customer will be responsible for reviewing and updating the Personnel Security policy every 3 years, and procedures annually. A successful control response will need to address the review and update process, including the role(s) responsible for initiating the review process, updating the policy and procedures, and providing approval of the updates.*> |

* + 1. Position Categorization (PS-2)

The organization:

1. Assigns a risk designation to all positions;
2. Establishes screening criteria for individuals filling those positions; and
3. Reviews and revises position risk designations [*FedRAMP* *Assignment: at least every three years*].

| PS-2 | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter PS-2(c): <*FedRAMP requirement: at least every 3 years*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| PS-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for assigning risk designations to all positions of customer personnel using Microsoft Azure that are consistent with the customer’s internal policies and procedures. A successful control response will need to address the criteria used in risk designation assignments (for example, specific responsibilities, access to certain types of data, etc.).*> |
| Part b | **Customer Responsibility**  <*The customer will be responsible for establishing screening criteria for individuals filling positions with access to Microsoft Azure. A successful control response will need to address the rationale for each level of screening based on the responsibilities or access associated with each risk designation.*> |
| Part c | **Customer Responsibility**  <*The customer will be responsible for reviewing and revising risk designations at the required frequency. A successful control response will need to address the review process, including the role(s) responsible for initiating the review process, revising risk designations, and providing approval of any changes.*> |

* + 1. Personnel Screening (PS-3)

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 5th year for top secret security clearance, the 10th year for secret security clearance, and 15th year for confidential security clearance. For moderate risk law enforcement and high impact public trust level, a reinvestigation is required during the 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 requirement: every 5th year for top secret security clearances, every 10th year for secret security clearances, every 15th year for confidential security clearances; every 5th year for moderate risk law enforcement and high impact public trust level*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| PS-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for screening individuals prior to authorizing access. A successful control response will need to demonstrate alignment of the screening as performed to the screening requirements established in PS-2.*> |
| Part b | **Customer Responsibility**  <*The customer will be responsible for rescreening individuals at the required frequency. A successful control response will need to discuss the process for initiating rescreening, as well as for disabling or removing access if rescreening is not completed in a timely manner.*> |

* + - 1. Control Enhancement PS-3 (3)

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 requirement: 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | | |

|  |
| --- |
| PS-3 (3) What is the solution and how is it implemented? |
| **Customer Responsibility**  <*The customer will be responsible for ensuring that access to information requiring special protection is contingent on additional screening as required by the specific nature of that information. A successful control response will need to address identifying such information and enforcing the additional screening prior to authorization of access.*> |

* + 1. Personnel Termination (PS-4)

The organization, upon termination of individual employment:

1. Disables information system access within [*FedRAMP Assignment: same day*];
2. Terminates/revokes any authenticators/credentials associated with the individual;
3. Conducts exit interviews that include a discussion of [*Assignment: organization-defined information security topics*];
4. Retrieves all security-related organizational information system-related property;
5. Retains access to organizational information and information systems formerly controlled by terminated individual; and
6. Notifies [*Assignment: organization-defined personnel or roles*] within [*Assignment: organization-defined time period*].

| PS-4 | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter PS-4(a): <*FedRAMP requirement: same day*> | |
| Parameter PS-4(c): <*Customer defined information security topics*> | |
| Parameter PS-4(f): <*Customer defined personnel or roles; 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| PS-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for disabling system access for terminated employees on the day of termination. A successful control response will need to address the process by which access disablement is requested, as well as the personnel responsible for initiating and completing the request.*> |
| Part b | **Customer Responsibility**  <*The customer will be responsible for terminating or revoking authenticators and credentials associated with terminated individuals. A successful control response will need to discuss the authenticators/credentials to be terminated/revoked, as well as the process for terminating or revoking each.*> |
| Part c | **Customer Responsibility**  <*The customer will be responsible conducting exit interviews. A successful control response will need to address the topics discussed during the interviews and the personnel responsible for conducting the interviews.*> |
| Part d | **Customer Responsibility**  <*The customer will be responsible for retrieving all security related, information system related, organizational property from terminated individuals. A successful control response will need to address the process and personnel responsible for ensuring that all such property is retrieved.*> |
| Part e | **Customer Responsibility**  <*The customer will be responsible for retaining access to information and information systems formerly controlled by terminated individuals. A successful control response will need to address how this retention occurs, personnel responsible for retention, and any minimum or maximum retention periods.*> |
| Part f | **Customer Responsibility**  <*The customer will be responsible for notifying relevant personnel within a defined time period after an individual is terminated. A successful control response will need to define the time period and personnel who should be notified, as well as discussing the process by which notification happens.*> |

* + 1. Personnel Transfer (PS-5)

The organization:

1. Reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization;
2. Initiates [*Assignment: organization-defined transfer or reassignment actions*] within [*Assignment: organization-defined time period following the formal transfer action*];
3. Modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and
4. Notifies [*Assignment: organization-defined personnel or roles*] within [*FedRAMP Assignment: within five days of the formal transfer action (DoD 24 hours)*].

| PS-5 | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter PS-5(b)-1: <*Customer defined transfer or reassignment actions*> | |
| Parameter PS-5(b)-2: <*Customer defined time period*> | |
| Parameter PS-5(d)-1: <*Customer defined personnel or roles*> | |
| Parameter PS-5(d)-2: <*FedRAMP requirement: within five days of the formal transfer action (DoD 24 hours)*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| PS-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for reviewing access authorizations for individuals when those individuals are reassigned or transferred. A successful control response will need to address the initiation of this review and individuals or roles responsible for performing and validating the results of reviews.*> |
| Part b | **Customer Responsibility**  <*The customer will be responsible for initiating reassignments or transfers within a customer-defined time period after the formal reassignment or transfer. A successful control response will need to address the specific actions taken, personnel responsible for those actions, and timeframes for initiation of those actions.*> |
| Part c | **Customer Responsibility**  <*The customer will be responsible for modifying access authorizations based on the results of the review carried out in part (a). A successful control response will need to address the process by which authorizations are modified, personnel responsible for initiating the change, and any technical means of enforcement of the change.*> |
| Part d | **Customer Responsibility**  <*The customer will be responsible for notifying relevant personnel within the required timeframe after a formal reassignment or transfer. A successful control response will need to address the identification of interested personnel or roles as well as the means by which notification occurs.*> |

* + 1. Access Agreements (PS-6)

The organization:

1. Develops and documents access agreements for organizational information systems;
2. Reviews and updates the access agreements [*FedRAMP Assignment: at least annually*]; and
3. Ensures that individuals requiring access to organizational information and information systems:
   1. Sign appropriate access agreements prior to being granted access; and
   2. Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or [*FedRAMP Assignment: at least annually*].

| PS-6 | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter PS-6(b): <*FedRAMP requirement: at least annually*> | |
| Parameter PS-6(c)(2): <*FedRAMP requirement: at least annually*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| PS-6 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for developing agreements for access to the system. A successful control response will need to outline the contents of access agreements and the conditions under which they are used.*> |
| Part b | **Customer Responsibility**  <*The customer will be responsible for reviewing and updating access agreements at the required frequency. A successful control response will need to address the initiation of the review process, the personnel or roles responsible for reviewing and updating the agreement, and the process for approval of any changes.*> |
| Part c | **Customer Responsibility**  <*The customer will be responsible for ensuring that individuals review and sign access agreements prior to initial access and to maintain access after updates. A successful control response will need to address the process for withholding access until after the initial signature is received, as well as for disabling or removing access if the access agreement changes and an individual does not re-sign it in a timely manner.*> |

* + 1. Third-Party Personnel Security (PS-7)

The organization:

1. Establishes personnel security requirements including security roles and responsibilities for third-party providers;
2. Requires third-party providers to comply with personnel security policies and procedures established by the organization;
3. Documents personnel security requirements;
4. Requires third-party providers to notify [*Assignment: organization-defined personnel or roles*] of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within [*FedRAMP Assignment: same day*]; and
5. Monitors provider compliance.

| PS-7 | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter PS-7(d)-1: <*Customer defined personnel or roles*> | |
| Parameter PS-7(d)-2: <*FedRAMP requirement: same day*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| PS-7 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for establishing personnel security requirements for third-party providers. A successful control response will need to outline these requirements and address the process for notifying third-party providers of the requirements.*> |
| Part b | **Customer Responsibility**  <*The customer will be responsible for requiring third-party providers to comply with the requirements established in part (a). A successful control response will need to address the process for obtaining agreement to the requirements and enforcing the requirements.*> |
| Part c | **Customer Responsibility**  <*The customer will be responsible for documenting personnel security requirements for third-party providers. A successful control response will need to discuss the process for creating documentation and sharing it with the providers.*> |
| Part d | **Customer Responsibility**  <*The customer will be responsible for including notification of terminations and transfers within the personnel security requirements. A successful control response will need to discuss the specific notification requirements, in particular the requirement for notification within the same day.*> |
| Part e | **Customer Responsibility**  <*The customer will be responsible for monitoring provider compliance with personnel security requirements. A successful control response will need to address personnel responsible for monitoring compliance, mechanisms used for monitoring, and consequences of non-compliance.*> |

* + 1. Personnel Sanctions (PS-8)

The organization:

1. Employs a formal sanctions process for personnel failing to comply with established information security policies and procedures; and
2. Notifies [*Assignment: organization-defined personnel or roles*] within [*Assignment: organization-defined time period*] when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

| PS-8 | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter PS-8(b)-1: <*Customer defined personnel or roles*> | |
| 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

|  |  |
| --- | --- |
| PS-8 What is the solution and how is it implemented? | |
| Part a | **Customer Responsibility**  <*The customer will be responsible for establishing a sanctions process for non-compliance with policies and procedures. A successful control response will need to address different forms of non-compliance and specific measures that may be enforced for each.*> |
| Part b | **Customer Responsibility**  <*The customer will be responsible for notifying interested personnel when the sanctions process is initiated. A successful control response will need to delineate the relevant personnel to be notified, the roles or individuals responsible for notification, and the information conveyed as part of the notification (to include at a minimum the individual sanctioned and the reason for the sanction).*> |

* 1. Risk Assessment (RA)
     1. Risk Assessment Policy and Procedures (RA-1)

The organization:

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

| RA-1 | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter RA-1(a): <*Customer-defined personnel or roles*> | |
| Parameter RA-1(b)(1): <*FedRAMP requirement: at least every 3 years*> | |
| Parameter RA-1(b)(2): <*FedRAMP requirement: 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) | |

| RA-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for developing, documenting, and disseminating Risk Assessment policy and procedures. A successful control response will need to address the content of the policy (which must include purpose, scope, roles, responsibilities, management commitment, coordination, and compliance) and procedures (which must facilitate the implementation of the policies and associated controls).*> |
| Part b | **Customer Responsibility**  <*The customer will be responsible for reviewing and updating the Risk Assessment policy every 3 years, and procedures annually. A successful control response will need to address the review and update process, including the role(s) responsible for initiating the review process, updating the policy and procedures, and providing approval of the updates.*> |

* + 1. Security Categorization (RA-2)

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 Authorizing Official 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| RA-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for categorizing the customer system and information contained within it. A successful control response will need to address the applicable Federal Laws, Executive Orders, directives, policies, regulations, standards, and guidance, as well as the key stakeholders involved in the categorization decision.*  *Resources related to information categorization include FIPS 199,* Standards for Security Categorization of Federal Information and Information Systems*, and NIST SP 800-60 Rev. 1,* Guide for Mapping Types of Information and Information Systems to Security Categories*.*> |
| Part b | **Customer Responsibility**  <*The customer will be responsible for documenting the security categorization. A successful control response will need to address supporting rationale, including types of information considered, risk impact analysis, and input from stakeholders and organizational officials.*> |
| Part c | **Customer Responsibility**  <*The customer will be responsible for presenting the security categorization decision to the Authorizing Official or a designated representative for review and approval.*> |

* + 1. Risk Assessment (RA-3)

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: at least every three years or when a significant change occurs*];
4. Disseminates risk assessment results to [*Assignment: organization-defined personnel or roles*]; and
5. Updates the risk assessment [*FedRAMP Assignment: at least every three years 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-3d Additional FedRAMP Requirements and Guidance:** **Requirement:** Requirement to include the Authorizing Official; for JAB authorizations to include FedRAMP.

| RA-3 | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter RA-3(b): <*FedRAMP requirement: Security Assessment Report*> | |
| Parameter RA-3(c): <*FedRAMP requirement: at least every three years or when a significant change occurs*> | |
| Parameter RA-3(d): <*Customer defined personnel or roles*> | |
| Parameter RA-3(e): <*FedRAMP requirement: at least every three years 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| RA-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for conducting a risk assessment, including a review of controls inherited from Microsoft Azure and those for which the customer is responsible. A successful control response will need to address the assessment methodology and calculation of the likelihood and magnitude of harm that could result from unauthorized access, use, disclosure, disruption, or modification of Microsoft Azure, the customer application, and the information processed, stored, and transmitted by those systems.*  *NIST SP 80-30 Rev. 1,* Guide for Conducting Risk Assessments*, and NIST SP 800-53A Rev. 4,* Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans *both provide guidance that may be used by the customer in developing the risk assessment methodology and performing the risk assessment.*> |
| Part b | **Customer Responsibility**  <*The customer will be responsible for documenting the results of the risk assessment in a Security Assessment Report. A successful control response will need to address specific requirements for the report (e.g., it should include controls that are considered “other than satisfied”, potential weaknesses in controls that meet minimum requirements, recommended remediation steps, and risks associated with the system). The customer may wish to employ a 3PAO to assist with the initial risk assessment (see CA-2).*> |
| Part c | **Customer Responsibility**  <*The customer will be responsible for reviewing risk assessment results at the required frequency. A successful control response will need to address the personnel or roles responsible for reviewing results, as well as any actions taken in response to risk assessment results.*> |
| Part d | **Customer Responsibility**  <*The customer will be responsible for disseminating risk assessment results to customer-defined stakeholders and organizational officials. A successful control response will need to outline the stakeholders involved and the means of distribution of results.*> |
| Part e | **Customer Responsibility**  <*The customer will be responsible for updating the risk assessment at the required frequency or when a significant change occurs. (Note that “significant change” is defined in NIST SP 800-37 Rev. 1, Appendix F.) A successful control response with need to discuss examples of significant changes that might occur within the customer application, as well as the specific actions that will be taken when the risk assessment is updated (such as updating system security plans and other documentation).*> |

* + 1. Vulnerability Scanning (RA-5)

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 days from date of discovery; moderate risk vulnerabilities mitigated within ninety 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

| RA-5 | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*>, Microsoft Azure | |
| Parameter RA-5(a): <*FedRAMP requirement: monthly for operating systems/infrastructure, web applications, and databases*> | |
| Parameter RA-5(d): <*FedRAMP requirement: high-risk vulnerabilities mitigated within thirty days from date of discovery; moderate risk vulnerabilities mitigated within ninety days from date of discovery*> | |
| Parameter RA-5(e): <*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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| RA-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for scanning for vulnerabilities in customer applications and databases. Additionally, IaaS customers using an operating system image not provided by Microsoft Azure will be responsible for scanning for vulnerabilities in the operating system. A successful control response will need to address the tools used to perform scans as well as the additional FedRAMP requirement for independent assessors to scan the system on an annual basis.*>  **Microsoft Azure**  Microsoft Azure implements the operating system portion of this control on behalf of PaaS customers. See section 15.14.4. |
| Part b | **Customer Responsibility**  <*The customer will be responsible for ensuring that vulnerability scanning tools use standards for enumerating components, flaws, and improper configurations; formatting checklists and test procedures; and measuring vulnerability impact. A successful control response will need to address how each vulnerability scanning tool in use meets these requirements (for example, by using Common Vulnerabilities and Exposures (CVE) values).*>  **Microsoft Azure**  Microsoft Azure implements the operating system portion of this control on behalf of PaaS customers. See section 15.14.4. |
| Part c | **Customer Responsibility**  <*The customer will be responsible for analyzing scan reports and assessment results for actionable data. A successful control response will need to address the roles or personnel responsible for the analysis, as well as criteria used in performing the analysis.*>  **Microsoft Azure**  Microsoft Azure implements the operating system portion of this control on behalf of PaaS customers. See section 15.14.4. |
| Part d | **Customer Responsibility**  <*The customer will be responsible for remediating vulnerabilities in customer applications and customer-provided OS images in accordance with the required timeframes. A successful control response will need to address prioritization of remediation activities and roles or personnel responsible for ensuring that timeframe requirements are met.*>  **Microsoft Azure**  Microsoft Azure implements the operating system portion of this control on behalf of PaaS customers. See section 15.14.4. |
| Part e | **Customer Responsibility**  <*The customer will be responsible for sharing vulnerability scan results and security assessment reports with customer-defined stakeholders. A successful control response will need to address the stakeholders involved and the types of information shared with each stakeholder.*>  **Microsoft Azure**  Microsoft Azure implements the operating system portion of this control on behalf of PaaS customers. See section 15.14.4. |

* + - 1. Control Enhancement RA-5 (1)

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 Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| RA-5 (1) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for scanning customer applications and customer-deployed OS images using compliant vulnerability scanning tools. A successful control response will need to address the specific tools used and the process required to update the list of information system vulnerabilities to be scanned for each.*>  **Microsoft Azure**  Microsoft Azure implements the operating system portion of this control on behalf of PaaS customers. See section 15.14.4.1. |

* + - 1. Control Enhancement RA-5 (2)

The organization updates the information system vulnerabilities scanned [*Selection (one or more):* [*FedRAMP* *Assignment: prior to a new scan*].

| RA-5 (2) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter RA-5(2): <*FedRAMP requirement: prior to a new scan*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| RA-5 (2) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for updating the list of vulnerabilities scanned prior to each scan. A successful control response will need to address the roles or personnel responsible for ensuring that this requirement is met, as well as the process for initiating a new scan if the required update does not occur.*>  **Microsoft Azure**  Microsoft Azure implements the operating system portion of this control on behalf of PaaS customers. See section 15.14.4.2. |

* + - 1. Control Enhancement RA-5 (3)

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 Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| RA-5 (3) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for ensuring that vulnerability scanning tools and procedures demonstrate the breadth and depth of coverage. A successful control response will need to address the specific tools in use and discuss the reason each tool is felt to provide sufficient breadth and depth of coverage.*>  **Microsoft Azure**  Microsoft Azure implements the operating system portion of this control on behalf of PaaS customers. See section 15.14.4.3. |

* + - 1. Control Enhancement RA-5 (5)

The organization includes privileged access authorization to [*FedRAMP Assignment: operating systems, databases, web applications*] for selected [*FedRAMP Assignment: all scans*].

| RA-5 (5) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter RA-5(5)-1: <*FedRAMP requirement: operating systems, databases, web applications*> | |
| Parameter RA-5(5)-2: <*FedRAMP requirement: 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| RA-5 (5) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for ensuring that scans of the customer environment include privileged access authorizations. A successful control response will need to address how privileged access authorizations are configured, as well as how successful authorization is validated during analysis of scan results.*>  **Microsoft Azure**  Microsoft Azure implements the operating system portion of this control on behalf of PaaS customers. See section 15.14.4.4. |

* + - 1. Control Enhancement RA-5 (6)

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

| RA-5 (6) | Control Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| RA-5 (6) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for using automated mechanisms to analyze vulnerability scan results over time to determine trends. A successful control response will need to discuss the mechanisms in use and the metrics employed in scan result analysis.*>  **Microsoft Azure**  Microsoft Azure implements the operating system portion of this control on behalf of PaaS customers. See section 15.14.4.5. |

* + - 1. Control Enhancement RA-5 (8)

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 Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| RA-5 (8) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for reviewing historic audit logs to determine if a vulnerability identified in the information system has been previously exploited. A successful control response will need to address the criteria used in analysis of audit logs to correlate log data with vulnerability scan results.*>  **Microsoft Azure**  Microsoft Azure implements the operating system portion of this control on behalf of PaaS customers. See section 15.14.4.6. |

* 1. System and Services Acquisition (SA)
     1. System and Services Acquisition Policy and Procedures (SA-1)

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:
3. System and services acquisition policy [*FedRAMP Assignment: at least every three years*]; and
4. System and services acquisition procedures [*FedRAMP Assignment: at least annually*].

| SA-1 | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter SA-1(a): <*Customer-defined personnel or roles*> | |
| Parameter SA-1(b)(1): <*FedRAMP requirement: at least every 3 years*> | |
| Parameter SA-1(b)(2): <*FedRAMP requirement: 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) | |

| SA-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for developing, documenting, and disseminating System and Services Acquisition policy and procedures. A successful control response will need to address the content of the policy (which must include purpose, scope, roles, responsibilities, management commitment, coordination, and compliance) and procedures (which must facilitate the implementation of the policies and associated controls).*> |
| Part b | **Customer Responsibility**  <*The customer will be responsible for reviewing and updating the Audit and Accountability policy every 3 years, and procedures annually. A successful control response will need to address the review and update process, including the role(s) responsible for initiating the review process, updating the policy and procedures, and providing approval of the updates.*> |

* + 1. Allocation of Resources (SA-2)

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: 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SA-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure**  Microsoft Azure implements this control on behalf of IaaS and PaaS customers. See section 14.15.2. |
| Part b | **Microsoft Azure**  Microsoft Azure implements this control on behalf of IaaS and PaaS customers. See section 14.15.2. |
| Part c | **Microsoft Azure**  Microsoft Azure implements this control on behalf of IaaS and PaaS customers. See section 14.15.2. |

* + 1. System Development Life Cycle (SA-3)

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: Microsoft Azure | |
| Parameter SA-3(a): <*Microsoft’s Security Development Lifecycle*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SA-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.15.3. |
| Part b | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.15.3. |
| Part c | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.15.3. |
| Part d | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.15.3. |

* + 1. Acquisitions Process (SA-4)

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:** The use of Common Criteria (ISO/IEC 15408) evaluated products is strongly preferred. See [http://www.niap-ccevs.org/vpl](https://www.microsoft.com/en-us/TrustCenter/Security/Identity) or [http://www.commoncriteriaportal.org/products.html](https://technet.microsoft.com/en-us/magazine/dn250023.aspx).

| SA-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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SA-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for including security functional requirements in acquisition contracts. A successful control response will need to address consideration of applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs in the creation of the contracts.*>  **Microsoft Azure**  Microsoft Azure implements this control for operating systems on behalf of PaaS customers. See section 15.15.4. |
| Part b | **Customer Responsibility**  <*The customer will be responsible for including security strength requirements in acquisition contracts. A successful control response will need to address consideration of applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs in the creation of the contracts.*>  **Microsoft Azure**  Microsoft Azure implements this control for operating systems on behalf of PaaS customers. See section 15.15.4. |
| Part c | **Customer Responsibility**  <*The customer will be responsible for including security assurance requirements in acquisition contracts. A successful control response will need to address consideration of applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs in the creation of the contracts.*>  **Microsoft Azure**  Microsoft Azure implements this control for operating systems on behalf of PaaS customers. See section 15.15.4. |
| Part d | **Customer Responsibility**  <*The customer will be responsible for including security-related documentation requirements in acquisition contracts. A successful control response will need to address consideration of applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs in the creation of the contracts.*>  **Microsoft Azure**  Microsoft Azure implements this control for operating systems on behalf of PaaS customers. See section 15.15.4. |
| Part e | **Customer Responsibility**  <*The customer will be responsible for including requirements for protecting security-related documentation in acquisition contracts. A successful control response will need to address consideration of applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs in the creation of the contracts.*>  **Microsoft Azure**  Microsoft Azure implements this control for operating systems on behalf of PaaS customers. See section 15.15.4. |
| Part f | **Customer Responsibility**  <*The customer will be responsible for including a description of the information system development environment and environment in which the system is intended to operate in acquisition contracts. A successful control response will need to address consideration of applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs in the creation of the contracts.*>  **Microsoft Azure**  Microsoft Azure implements this control for operating systems on behalf of PaaS customers. See section 15.15.4. |
| Part g | **Customer Responsibility**  <*The customer will be responsible for including acceptance criteria in acquisition contracts. A successful control response will need to address consideration of applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs in the creation of the contracts.*>  **Microsoft Azure**  Microsoft Azure implements this control for operating systems on behalf of PaaS customers. See section 15.15.4. |

* + - 1. Control Enhancement SA-4 (1)

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 Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SA-4 (1) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.15.4.1.  <*Hardware acquisition is inherited from Microsoft Azure*.> |

* + - 1. Control Enhancement SA-4 (2)

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: to include security-relevant external system interfaces and high-level design*]; [*Assignment: organization-defined design/implementation information*] at [*Assignment: organization-defined level of detail*].

| SA-4 (2) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: Microsoft Azure | |
| Parameter SA-4-1: <*security-relevant external system interfaces and high-level design*> | |
| Parameter SA-4-2: <*design and implementation information required by the SDL process*> | |
| Parameter SA-4-3: <*a level of detail sufficient for secure deployment*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SA-4 (2) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.15.4.2.  <*Hardware acquisition is inherited from Microsoft Azure*.> |

* + - 1. Control Enhancement SA-4 (8)

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 Enhancement Summary Information |
| --- | --- |
| Responsible Role: Microsoft Azure | |
| Parameter SA-4(8): <*standards specified in 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SA-4 (8) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*Customers are responsible for requiring the developer of customer-controlled software and operating systems to produce a plan for continuous monitoring of security control effectiveness. A successful control response will discuss the level of detail required by the customer as part of these continuous monitoring activities.*>  **Microsoft Azure**  Microsoft Azure implements this control for operating systems on behalf of PaaS customers. See section 15.15.4.3. |

* + - 1. Control Enhancement SA-4 (9)

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 Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SA-4 (9) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*Customers are responsible for requiring the developer of customer-controlled software and operating systems to identify required ports, protocols, services and functions early in the development process. A successful control response will address the process by which this requirement is enforced.*>  **Microsoft Azure**  Microsoft Azure implements this control for operating systems on behalf of PaaS customers. See section 15.15.4.4. |

* + - 1. Control Enhancement SA-4 (10)

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 Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SA-4 (10) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure**  Microsoft Azure does not implement PIV requirements for Government customers. As such, this control is not applicable. |

* + 1. Information System Documentation (SA-5)

The organization:

1. Obtains administrator documentation for the information system, system component, or information system service that describes:
   1. Secure configuration, installation, and operation of the system, component, or service;
   2. Effective use and maintenance of security functions/mechanisms; and
   3. Known vulnerabilities regarding configuration and use of administrative (i.e. privileged) functions;
2. Obtains user documentation for the information system, system component, or information system service that describes:
   1. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms;
   2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and
   3. User responsibilities in maintaining the security of the system, component, or service;
3. Documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and [*Assignment: organization-defined actions*] in response;
4. Protects documentation as required, in accordance with the risk management strategy; and
5. Distributes documentation to [*Assignment: organization-defined personnel or roles*].

| SA-5 | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: Microsoft Azure | |
| Parameter SA-5(c): <*Organization-defined actions*> | |
| Parameter SA-5(e): <*Developer, Tester 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SA-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*Customers are responsible for obtaining administrator documentation for customer-controlled software and operating systems. A successful control response will address the specific content requirements outlined in the control.*>  **Microsoft Azure**  Microsoft Azure implements this control for operating systems on behalf of PaaS customers. See section 15.15.5. |
| Part b | **Customer Responsibility**  <*Customers are responsible for obtaining user documentation for customer-controlled software and operating systems. A successful control response will address the specific content requirements outlined in the control.*>  **Microsoft Azure**  Microsoft Azure implements this control for operating systemson behalf of PaaS customers. See section 15.15.5. |
| Part c | **Customer Responsibility**  <*Customers are responsible for documenting attempts to obtain administrator and user documentation for customer-controlled software and operating systems if that documentation is not available. A successful control response will discuss the process by which attempts to obtain documentation are made as well as any additional actions taken.*>  **Microsoft Azure**  Microsoft Azure implements this control for operating systems on behalf of PaaS customers. See section 15.15.5. |
| Part d | **Customer Responsibility**  <*Customers are responsible for protecting administrator and user documentation for customer-controlled software and operating systems. A successful control response will discuss how the safeguards used are in accordance with the organization’s risk management strategy.*>  **Microsoft Azure**  Microsoft Azure implements this control for operating systems on behalf of PaaS customers. See section 15.15.5. |
| Part e | **Customer Responsibility**  <*Customers are responsible for distributing documentation for customer-controlled software and operating systems to appropriate personnel. A successful control response will discuss the means of distribution and the process for designating appropriate personnel or roles.*>  **Microsoft Azure**  Microsoft Azure implements this control for operating systems on behalf of PaaS customers. See section 15.15.5. |

* + 1. Security Engineering Principles (SA-8)

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: 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SA-8 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.15.6. |

* + 1. External Information System Services (SA-9)

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.

| SA-9 | Control Summary Information |
| --- | --- |
| Responsible Role: Microsoft Azure | |
| Parameter SA-9(a): <*FedRAMP Security Controls Baseline(s) if Federal information is processed or stored within the external system*> | |
| Parameter SA-9(c): <*Federal/FedRAMP Continuous Monitoring requirements must be met for external systems where Federal information is processed or stored*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SA-9 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.15.7. |
| Part b | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.15.7. |
| Part c | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.15.7. |

* + - 1. Control Enhancement SA-9 (1)

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 [*FedRAMP Assignment: see Additional Requirement and Guidance*].

|  |  |
| --- | --- |
| SA-9 (1) | Control Enhancement Summary Information |
| Responsible Role: Microsoft Azure | |
| Parameter SA-9(1)(b): <*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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SA-9 (1) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.15.7.1. |
| Part b | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.15.7.1. |

**SA-9 (1) Additional FedRAMP Requirements and Guidance:** **Requirement**: The service provider documents all existing outsourced security services and conducts a risk assessment of future outsourced security services. For JAB authorizations, future planned outsourced services are approved and accepted by the JAB.

| SA-9 (1) | Additional FedRAMP 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SA-9 (1) Additional: What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.15.7.1. |

* + - 1. Control Enhancement SA-9 (2)

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 Enhancement Summary Information |
| Responsible Role: Microsoft Azure | |
| Parameter SA-9(2): <*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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SA-9 (2) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.15.7.2. |

* + - 1. Control Enhancement SA-9 (4)

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 Enhancement Summary Information |
| Responsible Role: Microsoft Azure | |
| Parameter SA-9(4)-1: <*FedRAMP security requirements*> | |
| Parameter SA-9(4)-2: <*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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SA-9 (4) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.15.7.3. |

* + - 1. Control Enhancement SA-9 (5)

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*].

|  |  |
| --- | --- |
| SA-9 (5) | Control Enhancement Summary Information |
| Responsible Role: Microsoft Azure | |
| Parameter SA-9(5)-1: <*information processing, information data, and information services*> | |
| Parameter SA-9(5)-2: <*Microsoft Azure continental United States datacenters*> | |
| Parameter SA-9(5)-3: <*Microsoft Azure business requirements*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SA-9 (5) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.15.7.4. |

* + 1. Developer Configuration Management (SA-10)

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.

| SA-10 | Control Summary Information |
| --- | --- |
| Responsible Role: : Microsoft Azure | |
| Parameter SA-10(a): <*development, implementation, and operation*> | |
| Parameter SA-10(b): <*configuration items identified in CM-3*> | |
| Parameter SA-10(e): <*Microsoft Azure Security Operations*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SA-10 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for performing configuration management for customer-controlled operating systems and software. A successful control response will need to address the processes and mechanisms involved in configuration management.*>  **Microsoft Azure**  Microsoft Azure implements this control for operating systemson behalf of PaaS customers. See section 15.15.8. |
| Part b | **Customer Responsibility**  <*The customer will be responsible for documenting, managing, and controlling the integrity of changes to customer-controlled operating systems and software. A successful control response will need to address the processes and mechanisms involved these activities.*>  **Microsoft Azure**  Microsoft Azure implements this control for operating systems on behalf of PaaS customers. See section 15.15.8. |
| Part c | **Customer Responsibility**  <*The customer will be responsible for implementing only approved changes. A successful control response will need to address the approval process and safeguards in place to ensure only approved changes are implemented.*>  **Microsoft Azure**  Microsoft Azure implements this control for operating systemson behalf of PaaS customers. See section 15.15.8. |
| Part d | **Customer Responsibility**  <*The customer will be responsible for documenting approved changes customer-controlled operating systems and software as well as the potential security implications of such changes. A successful control response will need to discuss the process for documentation.*>  **Microsoft Azure**  Microsoft Azure implements this control for operating systemson behalf of PaaS customers. See section 15.15.8. |
| Part e | **Customer Responsibility**  <*The customer will be responsible for tracking, resolving, and reporting security flaws within customer-controlled operating systems and software. A successful control response will need to discuss the processes and tools used for tracking, resolution, and reporting.*>  **Microsoft Azure**  Microsoft Azure implements this control for operating systemson behalf of PaaS customers. See section 15.15.8. |

* + - 1. Control Enhancement SA-10 (1)

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 Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SA-10 (1) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for enabling integrity verification for customer-controlled operating systems and software. A successful control response will need to address the processes and mechanisms involved in integrity verification.*>  *<Red Hat container image signing provides a path to ensure authorship, integrity, and non-repudiation. Documentation can be found in the ‘Container Image Signing Integration Guide,’:*  [*https://access.redhat.com/articles/2750891*](https://access.redhat.com/articles/2750891)*>*  **Microsoft Azure**  Microsoft Azure implements this control for operating systemson behalf of PaaS customers. See section 15.15.8.1. |

* + 1. Developer Security Testing and Evaluation (SA-11)

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: Microsoft Azure | |
| Parameter SA-11(b)-1: <*tests required by the SDL process*> | |
| Parameter SA-11(b)-2: <*depth and coverage required by the SDL process*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SA-11 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for ensuring that the developer of customer-controlled operating systems and software creates and implements a security assessment plan. A successful control response will need to outline the security assessment plan.*>  **Microsoft Azure**  Microsoft Azure implements this control for operating systemson behalf of PaaS customers. See section 15.15.9. |
| Part b | **Customer Responsibility**  <*The customer will be responsible for ensuring that the developer of customer-controlled operating systems and software performs system testing at a customer-required depth and coverage. A successful control response will need to address the types of testing performed and the depth required.*>  **Microsoft Azure**  Microsoft Azure implements this control for operating systemson behalf of PaaS customers. See section 15.15.9. |
| Part c | **Customer Responsibility**  <*The customer will be responsible for ensuring that the developer of customer-controlled operating systems and software produces evidence of the execution of the security assessment plan and the results of the security testing/evaluation. A successful control response will need to address the process by which the customer obtains and reviews the evidence and results of testing.*>  **Microsoft Azure**  Microsoft Azure implements this control for operating systemson behalf of PaaS customers. See section 15.15.9. |
| Part d | **Customer Responsibility**  <*The customer will be responsible for ensuring that the developer of customer-controlled operating systems and software implements a verifiable flaw remediation process. A successful control response will need to outline the means by which flaws are identified and addressed.*>  **Microsoft Azure**  Microsoft Azure implements this control for operating systemson behalf of PaaS customers. See section 15.15.9. |
| Part e | **Customer Responsibility**  <*The customer will be responsible for ensuring that the developer of customer-controlled operating systems and software corrects flaws identified during security testing. A successful control response will need to discuss the procedure for identifying flaws, alerting appropriate personnel to correct flaws, and verifying the success of the correction.*>  **Microsoft Azure**  Microsoft Azure implements this control for operating systemson behalf of PaaS customers. See section 15.15.9. |

* + - 1. Control Enhancement SA-11 (1)

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:** (Requirement for SA-11 (1) or SA-11 (8) or both)**:** The service provider documents in the Continuous Monitoring Plan, how newly developed code for the information system is reviewed.

| SA-11 (1) | Control Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SA-11 (1) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for ensuring that the developer of customer-controlled operating systems and software employs static code analysis tools. A successful control response will need to discuss the tools in use, the means by which the tools are used to identify common flaws, and the process for documenting results of testing.*>  **Microsoft Azure**  Microsoft Azure implements this control for operating systemson behalf of PaaS customers. See section 15.15.9.1. |

* + - 1. Control Enhancement SA-11 (2)

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 Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SA-11 (2) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for ensuring that the developer of customer-controlled operating systems and software performs threat and vulnerability analysis and testing of the as-built system or software. A successful control response will need to address the analysis of how the as-built system differs from the initial design, as well as how any new vulnerabilities created as a result of these differences are reviewed and mitigated.*>  **Microsoft Azure**  Microsoft Azure implements this control for operating systemson behalf of PaaS customers. See section 15.15.9.2. |

* + - 1. Control Enhancement SA-11 (8)

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) Additional FedRAMP Requirements and Guidance:** **Requirement:** (Requirement for SA-11 (1) or SA-11 (8) or both): The service provider documents in the Continuous Monitoring Plan, how newly developed code for the information system is reviewed.

| SA-11 (8) | Control Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SA-11 (8) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for ensuring that the developer of customer-controlled operating systems and software employs dynamic code analysis tools. A successful control response will need to discuss the tools in use, the means by which the tools are used to identify common flaws, and the process for documenting results of testing.*>  **Microsoft Azure**  Microsoft Azure implements this control for operating systems on behalf of PaaS customers. See section 15.15.9.3. |

* 1. System and Communications Protection (SC)
     1. System and Communications Protection Policy and Procedures (SC-1)

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 every three years*]; and
   2. System and communications protection procedures [*FedRAMP Assignment: at least annually*].

| SC-1 | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter SC-1(a): <*Customer-defined personnel or roles*> | |
| Parameter SC-1(b)(1): <*FedRAMP requirement: at least every 3 years*> | |
| Parameter: SC-1(b)(2): <*FedRAMP requirement: 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) | |

| SC-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for developing, documenting, and disseminating System and Communications Protection policy and procedures. A successful control response will need to address the content of the policy (which must include purpose, scope, roles, responsibilities, management commitment, coordination, and compliance) and procedures (which must facilitate the implementation of the policies and associated controls).*> |
| Part b | **Customer Responsibility**  <*The customer will be responsible for reviewing and updating the System and Communications Protection policy every 3 years, and procedures annually. A successful control response will need to address the review and update process, including the role(s) responsible for initiating the review process, updating the policy and procedures, and providing approval of the updates.*> |

* + 1. Application Partitioning (SC-2)

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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SC-2 What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility** *<The customer is responsible for determining the functionality and access to their instance of Microsoft Azure components. Each customer can determine how they want to manage and implement access to their instance, and Microsoft does not have any responsibility in how the customer manages and implements access.>* |

* + 1. Information In Shared Resources (SC-4)

The information system prevents unauthorized and unintended information transfer via shared system resources.

| SC-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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SC-4 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.16.3. |

* + 1. Denial of Service Protection (SC-5)

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: Microsoft Azure | |
| Parameter SC-5-1: <*attacks on bandwidth, attacks on transactional capacity, attacks on storage capacity>* | |
| Parameter SC-5-2: <*geo-replication, IP address blocking, network-based DDoS protections>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SC-5 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure**  Microsoft Azure implements this control on behalf of both IaaS and PaaS customers. See section 14.16.4. |

* + 1. Resource Availability (SC-6)

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: Microsoft Azure | |
| Parameter: SC-6-1: <*processor and memory resources>* | |
| Parameter: SC-6-2: <*process priority, resource availability>* | |
| Parameter: SC-6-3: <*load balancing>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SC-6 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure**  Microsoft Azure implements this control on behalf of both IaaS and PaaS customers. See section 14.16.5. |

* + 1. Boundary Protection (SC-7)

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: Microsoft Azure | |
| Parameter SC-7(b): <*physically and logically>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SC-7 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both IaaS and PaaS customers. See section 14.16.6. |
| Part b | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both IaaS and PaaS customers. See section 14.16.6. |
| Part c | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both IaaS and PaaS customers. See section 14.16.6. |

* + - 1. Control Enhancement SC-7 (3)

The organization limits the number of external network connections to the information system.

| SC-7 (3) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: Microsoft Azur | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SC-7 (3) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure**  Microsoft Azure implements this control on behalf of both IaaS and PaaS customers. See section 14.16.6.1. |

* + - 1. Control Enhancement SC-7 (4)

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 annually*] and removes exceptions that are no longer supported by an explicit mission/business need.

| SC-7 (4) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: Microsoft Azure | |
| Parameter SC-7(4)(e): <*Annually>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SC-7 (4) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.16.6.2. |
| Part b | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.16.6.2.  . |
| Part c | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.16.6.2. |
| Part d | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.16.6.2. |
| Part e | **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.16.6.2. |

* + - 1. Control Enhancement SC-7 (5)

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 Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SC-7 (5) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure**  Microsoft Azure implements this control on behalf of both IaaS and PaaS customers. See section 14.16.6.3. |

* + - 1. Control Enhancement SC-7 (7)

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 Enhancement Summary Information |
| --- | --- |
| Responsible Role: Microsoft Azure | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SC-7 (7) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure**  Microsoft Azure implements this control on behalf of both IaaS and PaaS customers. See section 14.16.6.4. |

* + - 1. Control Enhancement SC-7 (8)

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 Enhancement Summary Information |
| --- | --- |
| Responsible Role: Microsoft Azure | |
| Parameter SC-7(8)(1): N/A | |
| Parameter SC-7(8)(2): N/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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SC-7 (8) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure**  This control is not applicable. See section 14.16.6.5. |

* + - 1. Control Enhancement SC-7 (12)

The organization implements [*Assignment: organization-defined host-based boundary protection mechanisms*] at [*Assignment: organization-defined information system components*].

| SC-7 (12) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: Microsoft Azure | |
| Parameter SC-7(12)-1: <*Packet Filtering, Firewalls>* | |
| Parameter SC-7(12)-2: <*All servers in the Microsoft Azure environment>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SC-7 (12) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure**  Microsoft Azure implements this control on behalf of both IaaS and PaaS customers. See section 14.16.6.6. |

* + - 1. Control Enhancement SC-7 (13)

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:** The service provider defines key information security tools, mechanisms, and support components associated with system and security administration and isolates those tools, mechanisms, and support components from other internal information system components via physically or logically separate subnets.

| SC-7 (13) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: Microsoft Azure | |
| Parameter SC-7(13)-1: <*see below>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SC-7 (13) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.16.6.7. |

* + - 1. Control Enhancement SC-7 (18)

The information system fails securely in the event of an operational failure of a boundary protection device.

| SC-7 (18) | Control Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SC-7 (18) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure**  Microsoft Azure implements this control on behalf of IaaS customers. See section 14.16.6.8. |

* + 1. Transmission Confidentiality and Integrity (SC-8)

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: <*confidentiality and integrity>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SC-8 What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility** *<Customers are responsible for configuring their web browsers, mobile devices, etc., to enable communications through FIPS 140-2 validated encryption. Customers who enforce FDCC/USGCB settings will achieve FIPS 140-2 encryption for data transmitted to Microsoft Azure and between their enablers and the Azure web services interface; strong encryption with FIPS-approved ciphers is still possible if workstations are not operating in FIPS mode.>* **Microsoft Azure** Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.16.7. |

* + - 1. Control Enhancement SC-8 (1)

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 Enhancement Summary Information |
| --- | --- |
| Responsible Role: Microsoft Azure | |
| Parameter SC-8(1)-1: <*Prevent unauthorized disclosure of information and detect changes to information>* | |
| Parameter SC-8(1)-2: <*A hardened or alarmed carrier Protective Distribution System (PDS)>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SC-8 (1) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure**  Microsoft Azure implements this control on behalf of IaaS customers. See section 14.16.7.1. |

* + 1. Network Disconnect (SC-10)

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 30 minutes for RAS-based sessions or no longer than 60 minutes for non-interactive user sessions*] of inactivity.

| SC-10 | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer* defined>, Microsoft Azure | |
| Parameter SC-10: <*30 minutes for RAS based session, 60 minutes for non-interactive sessions>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SC-10 What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  *<Microsoft Azure customers are responsible for implementing network disconnect for their owned and managed enclaves (e.g. specific Microsoft Azure services) that connect over non-Microsoft networks (e.g. customer owned and operated networks) to the Microsoft Azure accreditation environment.>*  **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.16.8. |

* + 1. Cryptographic Key Establishment & Management (SC-12)

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 cryptography

| SC-12 | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SC-12 What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  *<Government user entities will ensure that personal computing devices (client systems) are configured to request FIPS 140-2 encryption ciphers and protocols for all network sessions.>*  *<Red Hat Enterprise Linux 7, the underlying operating system for OpenShift, has achieved FIPS 140-2 certification. For documentation of certifications, please visit the US Government Certifications webpage:*  [*https://www.redhat.com/en/technologies/industries/government/standards*](https://www.redhat.com/en/technologies/industries/government/standards)*>* |

* + - 1. Control Enhancement SC-12 (2)

The organization produces, controls, and distributes symmetric cryptographic keys using [*FedRAMP* *Selection: NIST FIPS-compliant*] key management technology and processes.

| SC-12 (2) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter SC-12(2): <*FedRAMP requirement: 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SC-12 (2) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for producing, controlling, and distributing symmetric cryptographic keys (if any are used within the customer application) using NIST FIPS-compliant key management technology and processes. A successful control response will need to address the processes and tools used for key generation and discuss the reasons they are considered compliant.*>  *<To ensure OpenShift nodes generate x509 certificates utilizing FIPS-compliant algorithms, ensure the underling RHEL 7 hosts are configured to use FIPS. This can be accomplished by following CCE-80359-3, “Enable FIPS Mode in GRUB2”>* |

* + - 1. Control Enhancement SC-12 (3)

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 Enhancement Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter SC-12(3): <*Customer defines technology and processes*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SC-12 (3) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for producing, controlling, and distributing asymmetric cryptographic keys (if any are used within the customer application) using one of the specified tools or processes. A successful control response will need to address the processes and tools used for key generation and discuss the reasons they are considered compliant.*> |

* + 1. Use of Cryptography (SC-13)

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*> | |
| Parameter SC-13: <*FedRAMP requirement: 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SC-13 What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  *<OpenShift relies on the cryptographic services of the underlying operating system, Red Hat Enterprise Linux. To ensure RHEL is configured in FIPS mode, follow CCE-80359-3, “Enable FIPS Mode in GRUB2”>* |

* + 1. Collaborative Computing Devices (SC-15)

The information system:

1. Prohibits remote activation of collaborative computing devices with the following exceptions:[*FedRAMP Assignment: no exceptions*] and
2. Provides an explicit indication of use to users physically present at the devices.

| SC-15 | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter SC-15(a): <*FedRAMP requirement: 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SC-15 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for prohibiting remote activation of any collaborative computing devices within or controlled from the customer application.*> |
| Part b | **Customer Responsibility**  <*The customer will be responsible for providing an explicit indication of use of any collaborative computing devices within or controlled from the customer application. A successful control response will need to address how this explicit indication is enabled, the form it takes, and the means by which activation can be verified.*> |

**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 | Additional 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SC-15 What is the solution and how is it implemented? | |
| --- | --- |
| Req. 1 | **Customer Responsibility**  <*The customer will be responsible for providing easy to use functionality to disable any collaborative computing devices within or controlled from the customer application.*> |

* + 1. Public Key Infrastructure Certificates (SC-17)

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*> | |
| 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SC-17 What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for defining and enforcing a policy for issuing public key certificates, or else to obtain public key certificates from an approved service provider. A successful control response will need to outline the policy and address the mechanism by which the policy is enforced, or else discuss the approved service provider and the process by which certificates are obtained.*> |

* + 1. Mobile Code (SC-18)

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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SC-18 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*Mobile code is code that is downloaded and executed by the client machine, rather than on the remote host. The customer will be responsible for defining mobile code technologies as acceptable or unacceptable for use within the system.*> |
| Part b | **Customer Responsibility**  <*The customer will be responsible for defining usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies.*> |
| Part c | **Customer Responsibility**  <*The customer will be responsible for authorizing, monitoring, and controlling the use of mobile code within the system.*> |

* + 1. Voice Over Internet Protocol (SC-19)

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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SC-19 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for establishing usage restrictions and implementation guidance for the use of VoIP technologies within the customer application. A successful control response will need to address whether and how VoIP technologies are used and outline the conditions under which that usage is appropriate.*> |
| Part b | **Customer Responsibility**  <*The customer will be responsible for authorizing, monitoring, and controlling the use of VoIP within the system.*> |

* + 1. Secure Name / Address Resolution Service (Authoritative Source) (SC-20)

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: None – Not Applicable | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SC-20 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure**  OMB Memorandum 08-23 specifies that DNS providers must take certain actions to protect .gov domains. Microsoft does not resolve .gov domain names for Federal users, so this control is not applicable. |
| Part b | **Microsoft Azure**  OMB Memorandum 08-23 specifies that DNS providers must take certain actions to protect .gov domains. Microsoft does not resolve .gov domain names for Federal users, so this control is not applicable. |

* + 1. Secure Name / Address Resolution Service (Recursive or Caching Resolver) (SC-21)

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: 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SC-21 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.16.16. |

* + 1. Architecture and Provisioning for Name-Address Resolution Service (SC-22)

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: Microsoft Azure | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SC-22 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure**  Microsoft Azure implements this control on behalf of both PaaS and IaaS customers. See section 14.16.17. |

* + 1. Session Authenticity (SC-23)

The information system protects the authenticity of communications sessions.

| SC-23 | 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SC-23 What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for guarding against, for example, man in the middle or session hijacking attacks for connections to the customer application, for example via the use of TLS. A successful control response will address the various types of attacks against session authenticity and the mechanisms used to protect against those attacks.*> |

* + 1. Protection of Information at Rest (SC-28)

The information system protects the [*FedRAMP* *Selection: confidentiality AND integrity]*] of [*Assignment: organization-defined information at rest*].

**SC-28 Additional FedRAMP Requirements and Guidance:** **Requirement:** 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: confidentiality and integrity | |
| Parameter SC-28-2: customer data | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SC-28 What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for controlling access to their Azure Storage Account Keys. In addition, customers may choose to encrypt data prior to saving it in their Azure Storage accounts. A successful control response will need to address these and any other means by which the customer protects information at rest.*>  **Microsoft Azure**  Microsoft Azure also protects customer information at rest using physical and logical access controls and multiple CRC checks at every data handoff. |

* + - 1. Control Enhancement SC-28 (1)

The information system implements cryptographic mechanisms to prevent unauthorized disclosure and modification of [*Assignment: organization-defined information*] on [*Assignment: organization-defined information system components*]

| SC-28 (1) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*>, Microsoft Azure | |
| Parameter SC-28(1)-1: customer data | |
| Parameter SC-28(1)-2: Microsoft Azure servers | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination:  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SC-28 (1) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for controlling access to their Azure Storage Account Keys. In addition, customers may choose to encrypt data prior to saving it in their Azure Storage accounts. A successful control response will need to address these and any other means by which the customer protects information at rest.*>  **Microsoft Azure**  Microsoft Azure protects the confidentiality and integrity of customer data on Microsoft Azure servers using the information-handling procedures outlined in SC-28. |

* + 1. Process Isolation (SC-39)

The information system maintains a separate execution domain for each executing process.

| SC-39 | 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SC-39 What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure**  All 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 |

* 1. System and Information Integrity (SI)
     1. System and Information Integrity Policy and Procedures (SI-1)

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 every three years*]; and
   2. System and information integrity procedures [*FedRAMP Assignment: at least annually*].

| SI-1 | Control Summary Information |
| --- | --- |
| Responsible Role: <*Customer defined*> | |
| Parameter SI-1(a): <*Customer-defined personnel or roles*> | |
| Parameter SI-1(b)(1): <*FedRAMP requirement: at least every 3 years*> | |
| Parameter SI-1(b)(2): <*FedRAMP requirement: 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) | |

| SI-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for developing, documenting, and disseminating System and Information Integrity policy and procedures. A successful control response will need to address the content of the policy (which must include purpose, scope, roles, responsibilities, management commitment, coordination, and compliance) and procedures (which must facilitate the implementation of the policies and associated controls).*> |
| Part b | **Customer Responsibility**  <*The customer will be responsible for reviewing and updating the System and Information Integrity policy every 3 years, and procedures annually. A successful control response will need to address the review and update process, including the role(s) responsible for initiating the review process, updating the policy and procedures, and providing approval of the updates.*> |

* + 1. Flaw Remediation (SI-2)

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: Within 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*> | |
| Parameter SI-2(c): FedRAMP Requirement: [Within 30 days of release of updates] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SI-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Customer Responsibility  <*The customer will be responsible for analyzing their applications for flaws, reporting on those flaws, and correcting them. A successful control response will include a discussion of the process by which flaws are discovered and remediated, as well as tools that are used to assist in detection and remediation.*  *Azure provides tools to assist with identifying flaws such as missing updates or OS configurations that do not meet the recommended baselines. Please see the Security Center Intro at* [*https://azure.microsoft.com/en-us/documentation/articles/security-center-intro/*](https://azure.microsoft.com/en-us/documentation/articles/security-center-intro/) *for more information.*>  **Microsoft Azure**  Microsoft Azure implements this requirement for OS images on behalf of PaaS customers. See section 15.17.2. |
| Part b | Customer Responsibility  *<The customer will be responsible for testing application updates related to flaw remediation prior to installation. A successful control response will discuss the testing process (e.g. the nature of the test environment, the types of testing performed, the tools used in testing, etc.).>*  **Microsoft Azure**  Microsoft Azure implements this requirement for OS images on behalf of PaaS customers. See section 15.17.2. |
| Part c | Customer Responsibility  *<The customer will be responsible for installing security-relevant software updates to their application within 30 days of the release of those updates. A successful control response will detail how the customer ensures that this update schedule can be met while still performing sufficient testing.>*  **Microsoft Azure**  Microsoft Azure implements this requirement for OS images on behalf of PaaS customers. See section 15.17.2. |
| Part d | Customer Responsibility  *<The customer will be responsible for incorporating flaw remediation activities into their organizational configuration management process. A successful control response will address how flaws are categorized in terms of the types of changes that are subject to configuration management, as well as the approval process for remediation activities (see the CM family of controls).>* |

* + - 1. Control Enhancement SI-2 (2)

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 Enhancement Summary Information |
| --- | --- |
| Responsible Role: *<Customer defined>* | |
| Parameter SI-2(2): <*FedRAMP Requirement: Monthly*> | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SI-2 (2) What is the solution and how is it implemented? |
| --- |
| Customer Responsibility  *<The customer will be required to employ automated mechanisms on a monthly basis to determine the state of information system components with regard to flaw remediation on their information systems as required by their organization’s security policy. A successful response will address the customer’s use of automated tools such as Nessus to preform periodic and on-demand scans through their system to determine the state of system compenents with regard to flaw remediation.>* |

* + - 1. Control Enhancement SI-2 (3)

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 Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SI-2 (3) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  *<The customer is responsible for scanning for flaws in their information systems and for measuring the time between flaw identification and flaw remediation. A successful control response will need to address the time between flaw identification and remediation using timestamps and calculates the time elapsed difference.>* |
| Part b | **Customer Responsibility**  *<The customer will be responsible for scanning for flaws in their information systems and for establishing benchmarks for taking corrective actions according to their organizational policies. A successful control response will need to address the use of benchmarks to remediate high, and moderate risk flaws within a customer defined period after a flaws discovery>* |

* + 1. Malicious Code Protection (SI-3)

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 alerting administrator or defined security personnel*] 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 Requirement: weekly*> | |
| Parameter SI-3(c)(1)-2: <*FedRAMP Requirement: includes endpoints*> | |
| Parameter SI-3(c)(2): <*FedRAMP Requirement: to include alerts to administrator or defined 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SI-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  *<The customer is responsible for ensuring that that they employ malicious code protection at information system entry, and exit points to detect and eradicate malicious code.. A successful control response will need to address use of code protection mechinisms to protect assests from malicious software (ie, Viruses, malware, rootkits, worms, and scripts).>* |
| Part b | **Customer Responsibility**  *<The customer is responsible for ensuring that they update their malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures. A successful control response will need to address that the protection mechinisms stated in part-a of this control are updated when a new version or definition release becomes available.>* |
| Part c | **Customer Responsibility**  *<The customer is responsible for ensuring that they configure their malicious code protection mechanisms will preform periodic scans on a weekly basis. The customer will preform real-time scans of files from all external sources, including endpoints as the files are downloaded, opened, or executed in accordance with organizational security policy. The customer will also send alerts to an administrator or another defined security personnel in response to detected malicious code.>* |
| Part d | **Customer Responsibility**  *<The customer is responsible for addressing the receipt of false positives during malicious code detation and eradication. These fasle positives will report potential impact of the availability of the information system. A succsessfull control response will detail the steps taken when false positives are detected within the system with the resulting impact of availability to the information system*.> |

* + - 1. Control Enhancement SI-3 (1)

The organization centrally manages malicious code protection mechanisms.

| SI-3 (1) | Control Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SI-3 (1) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  *<The customer is responsible for ensuring that their malicious code protection mechanisms are centrally managed. A successful control response will need to address that the planning, implementing, assessing, authorizing and monitoring of their malicious code protection mechanism is centered in one location.>* |

* + - 1. Control Enhancement SI-3 (2)

The information system automatically updates malicious code protection mechanisms.

| SI-3 (2) | Control Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SI-3 (2) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  *<The customer is responsible for ensuring that they update their malicious code protection mechanisms automatically when new versions/defintions become avaliable. A successful control response will need to address that the employed malicious code protection mechanisms definitions are configured to be updated automatically.>* |

* + - 1. Control Enhancement SI-3 (7)

The information system implements nonsignature-based malicious code detection mechanisms.

| SI-3 (7) | Control Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SI-3 (7) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  *<The customer is responsible for ensuring that they implement a nonsignature-based malicious code detection mechanism on their information system. A successful control response will need to address a nonsignature based detection mechanism that can detect, analyze and describe the characteristics or behavior of malicious code and could provide safeguards against malicious code for which signatures do not yet exist.>* |

* + 1. Information System Monitoring (SI-4)

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; and
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 | Control Summary Information |
| --- | --- |
| Responsible Role: Microsoft Azure | |
| Parameter SI-4(a)(1): *<Ensure the proper functioning of internal processes and controls in furtherance of regulatory and compliance requirements; examine system records to confirm that the system is functioning in an optimal, resilient, and secure state; identify irregularities or anomalies that are indicators of a system malfunction or compromise>* | |
| Parameter SI-4(b): *<Microsoft Azure SLAM (Security Logging and Auditing) and OSSC logging and monitoring>* | |
| Parameter SI-4(g)-1: *<Monitoring aligned with SI-4(a)>* | |
| Parameter SI-4(g)-2: *<Service Engineer Operations>* | |
| Parameter SI-4(g)-3: *<Daily and as needed>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SI-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Microsoft Azure implements this control on behalf of IaaS. See section 14.17.4. |
| Part b | Microsoft Azure implements this control on behalf of IaaS. See section 14.17.4. |
| Part c | Microsoft Azure implements this control on behalf of IaaS. See section 14.17.4. |
| Part d | Microsoft Azure implements this control on behalf of IaaS. See section 14.17.4. |
| Part e | Microsoft Azure implements this control on behalf of IaaS. See section 14.17.4. |
| Part f | Microsoft Azure implements this control on behalf of IaaS. See section 14.17.4. |
| Part g | Microsoft Azure implements this control on behalf of IaaS. See section 14.17.4. |

* + - 1. Control Enhancement SI-4 (1)

The organization connects and configures individual intrusion detection tools into an information system-wide intrusion detection system.

| SI-4 (1) | Control Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SI-4 (1) What is the solution and how is it implemented? |
| --- |
| Microsoft Azure implements this control on behalf of IaaS. See section 14.17.4.1. |

* + - 1. Control Enhancement SI-4 (2)

The organization employs automated tools to support near real-time analysis of events.

| SI-4 (2) | Control Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SI-4 (2) What is the solution and how is it implemented? |
| --- |
| Microsoft Azure implements this control on behalf of IaaS. See section 14.17.4.2. |

* + - 1. Control Enhancement SI-4 (4)

The information system monitors inbound and outbound communications traffic [*FedRAMP Assignment:* *continually]* for unusual or unauthorized activities or conditions.

| SI-4 (4) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: Microsoft Azure | |
| Parameter SI-4(4): FedRAMP Requirement: [continually] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SI-4 (4) What is the solution and how is it implemented? |
| --- |
| Microsoft Azure implements this control on behalf of IaaS. See section 14.17.4.3. |

* + - 1. Control Enhancement SI-4 (5)

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 Enhancement Summary Information |
| --- | --- |
| Responsible Role: Microsoft Azure | |
| Parameter SI-4(5)-1: *<Personnel defined in the Incident Response plan>* | |
| Parameter SI-4(5)-2: *<Criteria defined in the Incident Response plan>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SI-4 (5) What is the solution and how is it implemented? |
| --- |
| Microsoft Azure implements this control on behalf of IaaS. See section 14.17.4.4. |

* + - 1. Control Enhancement SI-4 (14)

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 Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SI-4 (14) What is the solution and how is it implemented? |
| --- |
| Microsoft Azure implements this control on behalf of IaaS. See section 14.17.4.5. |

* + - 1. Control Enhancement SI-4 (16)

The organization correlates information from monitoring tools employed throughout the information system.

| SI-4 (16) | Control Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SI-4 (16) What is the solution and how is it implemented? |
| --- |
| Microsoft Azure implements this control on behalf of IaaS. See section 14.17.4.6. |

* + - 1. Control Enhancement SI-4 (23)

The organization implements [*Assignment: organization-defined host-based monitoring mechanisms*] at [*Assignment: organization-defined information system components*].

| SI-4 (23) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: Microsoft Azure | |
| Parameter SI-4(23)-1: *<Windows Event Logging>* | |
| Parameter SI-4(23)-2: *<all hosts>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SI-4 (23) What is the solution and how is it implemented? |
| --- |
| Microsoft Azure implements this control on behalf of IaaS. See section 14.17.4.7. |

* + 1. Security Alerts, Advisories, and Directives (SI-5)

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: Microsoft Azure | |
| Parameter SI-5(a): FedRAMP Requirement: [includes US-CERT] | |
| Parameter SI-5(c): FedRAMP Requirement: [includes OSSC, OSSC-SIM, Microsoft Azure Security and Compliance, WALS, Patch Triage Team, RDOS Team, MA SQL DB teams] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SI-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for receiving relevant security alerts, advisories and directives. A successful control response will need to discuss the external sources of security alerts, advisories, and directives (including US-CERT as required by FedRAMP).*>  **Microsoft Azure**  Microsoft Azure implements this control for operating systems on behalf of PaaS customers. See section 15.17.5. |
| Part b | **Customer Responsibility**  <*The customer will be responsible for generating internal security alerts, advisories and directives. A successful control response will need to address the criteria used to determine what alerts, advisories, and directives are necessary, based on the specifics of the customer’s mission, software, or service.*>  **Microsoft Azure**  Microsoft Azure implements this control for operating systems on behalf of PaaS customers. See section 15.17.5. |
| Part c | **Customer Responsibility**  <*The customer will be responsible for disseminating security alerts, advisories and directives within the customer organization and to external organizations as necessary. A successful control response will need to address the personnel or roles within the organization who require notification.*>  **Microsoft Azure**  Microsoft Azure implements this control for operating systems on behalf of PaaS customers. See section 15.17.5. |
| Part d | **Customer Responsibility**  <*The customer will be responsible for implementing security directives within customer-controlled operating systems, software, and services. A successful control response will need to address how the organization meets established time frames for implementing security directives.*>  **Microsoft Azure**  Microsoft Azure implements this control for operating systems on behalf of PaaS customers. See section 15.17.5. |

* + 1. Security Functionality Verification (SI-6)

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: Microsoft Azure | |
| Parameter SI-6(a): *< See below >* | |
| Parameter SI-6(b): FedRAMP Requirement: [Upon system start up, restart, and continuously as described below] | |
| Parameter SI-6(c): FedRAMP Requirement: [service engineer personnel] | |
| Parameter SI-6(d)-1: *<initiates the Incident Response process>* | |
| Parameter SI-6(d)-2: FedRAMP Requirement: [notify 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

|  |  |
| --- | --- |
| SI-6 What is the solution and how is it implemented? | |
| Part a | **Customer Responsibility**  <*The customer will be responsible for verifying the correct operation of security functions within customer-controlled operating systems and software. A successful control response will need to discuss the security functions deemed necessary to verify, as well as the means for testing the correct operation and resolving any issues found.*>  **Microsoft Azure**  Microsoft Azure implements portions of this control on behalf of both IaaS and PaaS customers. See section 14.17.6. |
| Part b | **Customer Responsibility**  <*The customer will be responsible for performing security function verification at customer-specified frequencies and under customer-specified circumstances (to include the requirements stated by FedRAMP). A successful control response will need to address the rationale for selection of the specific frequency and circumstances of security function verification.*>  **Microsoft Azure**  Microsoft Azure implements portions of this control on behalf of both IaaS and PaaS customers. See section 14.17.6. |
| Part c | **Customer Responsibility**  <*The customer will be responsible for notifying appropriate personnel of failed security verification tests. A successful control response will need to outline the personnel or roles selected (to include system administrators and security personnel as required by FedRAMP).*>  **Microsoft Azure**  Microsoft Azure implements portions of this control on behalf of both IaaS and PaaS customers. See section 14.17.6. |
| Part d | **Customer Responsibility**  <*The customer will be responsible for performing appropriate actions in response to anomalies in security function verification. A successful control response will need to discuss the actions taken (to include notification of system administrators and security personnel as required by FedRAMP) as well as the rationale for selecting these actions.*>  **Microsoft Azure**  Microsoft Azure implements portions of this control on behalf of both IaaS and PaaS customers. See section 14.17.6. |

* + 1. Software & Information Integrity (SI-7)

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: Microsoft Azure | |
| Parameter SI-7: *<software, firmware 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SI-7 What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for employing integrity verification tools for customer-controlled operating systems and software. A successful control response will need to discuss the tools in use and the integrity-checking mechanisms these tools employ.*>  **Microsoft Azure**  Microsoft Azure implements this control for operating systems on behalf of PaaS customers. See section 15.17.7. |

* + - 1. Control Enhancement SI-7 (1)

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 Enhancement Summary Information |
| --- | --- |
| Responsible Role: Microsoft Azure | |
| Parameter SI-7(1)-1: *< software and information >* | |
| Parameter SI-7(1)-2: FedRAMP Requirement:[ at deployment, continually ] | |
| Parameter SI-7(1)-3: FedRAMP Requirement:[ Monthly ] | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SI-7 (1) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for performing integrity checks at customer-specified frequencies and under customer-specified circumstances (including frequencies and circumstances specified by FedRAMP). A successful control response will need to identify the criteria for performing integrity checking, as well as the rationale for selecting those criteria.*>  **Microsoft Azure**  Microsoft Azure implements this control for operating systems on behalf of PaaS customers. See section 15.17.7.1. |

* + - 1. Control Enhancement SI-7 (7)

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 Enhancement Summary Information |
| --- | --- |
| Responsible Role: Microsoft Azure | |
| Parameter SI-7(7): *<changes to operating system files, installation of software, privilege elevation>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SI-7 (7) What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for incorporating the detection of customer-defined security-relevant changes into the customer’s incident response capability. A successful control response will need to outline the process for deeming particular changes as security-relevant and the means by which the incident response capability is invoked when needed.*>  **Microsoft Azure**  Microsoft Azure implements this control for operating systems on behalf of PaaS customers. See section 15.17.7.2. |

* + 1. Spam Protection (SI-8)

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 policy and procedures.

| SI-8 | 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SI-8 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Microsoft Azure**  Currently, Microsoft Azure does not host mail servers for its customers, thus spam protection is not applicable. |
| Part b | **Microsoft Azure**  Currently, Microsoft Azure does not host mail servers for its customers, thus spam protection is not applicable. |

* + - 1. Control Enhancement SI-8 (1)

The organization centrally manages spam protection mechanisms.

| SI-8 (1) | Control Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SI-8 (1) What is the solution and how is it implemented? |
| --- |
| **Microsoft Azure**  Currently, Microsoft Azure does not host mail servers for its customers, thus spam protection is not applicable. |

* + - 1. Control Enhancement SI-8 (2)

The organization automatically updates spam protection mechanisms.

| SI-8 (2) | Control Enhancement 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

|  |
| --- |
| SI-8 (2) What is the solution and how is it implemented? |
| **Microsoft Azure**  Currently, Microsoft Azure does not host mail servers for its customers, thus spam protection is not applicable. |

* + 1. Information Input Validation (SI-10)

The information system checks the validity of [*Assignment: organization-defined information inputs*].

| SI-10 | Control Summary Information |
| --- | --- |
| Responsible Role: Microsoft Azure | |
| Parameter SI-10: *<all information inputs>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SI-10 What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for checking the validity of information inputs to customer-controlled operating systems and software. A successful control response will need to discuss the specific inputs for which the validity is checked, the rationale for selecting those inputs for validity checking, and the response taken by the system to invalid inputs.*>  **Microsoft Azure**  Microsoft Azure implements this control for operating systems on behalf of PaaS customers. See section 15.17.9. |

* + 1. Error Handling (SI-11)

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: Microsoft Azure | |
| Parameter SI-11(b): *<authorized service personnel and Microsoft Azure users>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SI-11 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | **Customer Responsibility**  <*The customer will be responsible for generating error messages in customer-controlled operating systems and software that provide information necessary for corrective actions without revealing information that could be exploited by adversaries. A successful control response will need to discuss the process by which error messages are created, analyzed, and corrected when necessary.*>  **Microsoft Azure**  Microsoft Azure implements this control for operating systems on behalf of PaaS customers. See section 15.17.10. |
| Part b | **Customer Responsibility**  <*The customer will be responsible for revealing error messages only to authorized personnel. A successful control response will need to address how error messages are displayed and the means by which access to error messages is controlled.*>  **Microsoft Azure**  Microsoft Azure implements this control for operating systems on behalf of PaaS customers. See section 15.17.10. |

* + 1. Information Output Handling and Retention (SI-12)

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: 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 Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SI-12 What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  <*The customer will be responsible for handling and retaining information within customer-controlled systems and software in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements. A successful control response will need to outline the specific requirements applicable to customer information handling and retention, and the means by which those requirements are met.*>  **Microsoft Azure**  Microsoft Azure implements portions of this control on behalf of PaaS customers. See section 15.17.11. |

* + 1. Memory Protection (SI-16)

The information system implements [*Assignment: organization-defined security safeguards*] to protect its memory from unauthorized code execution.

| SI-16 | Control Summary Information |
| --- | --- |
| Responsible Role: Microsoft Azure | |
| Parameter SI-16: *<Windows protections, including No Execute, Address Space Layout Randomization, and Data Execution Prevention>* | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing Provisional Authority to Operate (P-ATO) for Microsoft Azure | |

| SI-16 What is the solution and how is it implemented? |
| --- |
| **Customer Responsibility**  Memory and unauthorized code protection mechanisms are provided in the base operating system, Red Hat Enterprise Linux. This includes buffer overflow protection, execution of code on a process’ or thread’s stack, modification of a function return address on the process’ or threads stack to jump to previously known processor instructions, and modification of process section other than the segment that holds compile time initialized data and segment holding the mapping of all uninitialized variables. For the runtime instances of binaries, all user-provided applications and their depending libraries that are compiled and linked with the following properties: (1) presence of the ELF program header entry of PT\_GNU\_STACK and the absence of the PF\_X bit in the p\_flags ELF header flags; (2) presence of the ELF program header entry of PT\_GNU\_RELRO with memory range information covering the following ELF sections: .tdata, .preinit\_array, .init\_array, .fini\_array, .ctors, .dtors, .data.rel.ro, .dynamic, .got including .got.plt. The secure state implied with this functionality covers the following aspects where the following list explains the implication of each bullet above:   * + 1. When exploiting buffer overruns of an application, the attacker cannot feed code onto the stack and execute it.     2. When exploiting buffer overruns of an application, the modify of the return addresses stored on a stack jump to a previously known code segment is much harder to achieve by an attacker. Due to the address randomization, any memory address of code already present with the application or loaded libraries will be different with each startup of the application.     3. The ELF header sections listed above are set read-only using the mprotect system call by the loaded before the application gains control. When exploiting buffer overruns, the attacker cannot modify information in those memory sections. These sections store offset tables required for the dynamic linking mechanism and, if abused, allow attackers to modify the jump addresses of object accesses. Full protection against this type of attack can only be achieved if the application and all depending shared libraries are compiled linked with full protection enabled. When at least one shared libraroy the application depends on or the application itself is compiled and linked with partial protection, only partial protection against this type of attack is available for the given application.   To enforce functionality in bullet a), /proc/sys/kernel/exec-shield must contain either a 1 or 2.  To enforce the functionality in bullet b), /proc/sys/kernel/randomize\_va\_space must contain a 2 (1 implies the address randomization is enabled except for the brk system call).  For full documentation on common criteria evaluated memory protections, Red Hat publishes full common criteria paperwork online:  <https://www.redhat.com/en/technologies/industries/government/standards>> |