

NIST Controls and PCF[®] Documentation

Published: 22 Mar 2019

Table of Contents

Table of Contents	2
Assessment of Pivotal Cloud Foundry against NIST SP 800-53(r4) Controls	8
AC - Access Control Control Family	9
AC-1 ACCESS CONTROL POLICY AND PROCEDURES	10
AC-2 ACCOUNT MANAGEMENT	11
AC-3 ACCESS ENFORCEMENT	13
AC-4 INFORMATION FLOW ENFORCEMENT	14
AC-5 SEPARATION OF DUTIES	15
AC-6 LEAST PRIVILEGE	16
AC-7 UNSUCCESSFUL LOGON ATTEMPTS	17
AC-8 SYSTEM USE NOTIFICATION	18
AC-9 PREVIOUS LOGON (ACCESS) NOTIFICATION	19
AC-10 CONCURRENT SESSION CONTROL	20
AC-11 SESSION LOCK	21
AC-12 SESSION TERMINATION	22
AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION	23
AC-16 SECURITY ATTRIBUTES	24
AC-17 REMOTE ACCESS	25
AC-18 WIRELESS ACCESS	26
AC-19 ACCESS CONTROL FOR MOBILE DEVICES	27
AC-20 USE OF EXTERNAL INFORMATION SYSTEMS	28
AC-21 INFORMATION SHARING	29
AC-22 PUBLICLY ACCESSIBLE CONTENT	30
AC-23 DATA MINING PROTECTION	31
AC-24 ACCESS CONTROL DECISIONS	32
AC-25 REFERENCE MONITOR	33
AU - Audit and Accountability Control Family	34
AU-1 AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES	35
AU-2 AUDIT EVENTS	36
AU-3 CONTENT OF AUDIT RECORDS	37
AU-4 AUDIT STORAGE CAPACITY	38
AU-5 RESPONSE TO AUDIT PROCESSING FAILURES	39
AU-6 AUDIT REVIEW, ANALYSIS, AND REPORTING	40
AU-7 AUDIT REDUCTION AND REPORT GENERATION	41
AU-8 TIME STAMPS	42
AU-9 PROTECTION OF AUDIT INFORMATION	43
AU-10 NON-REPUDIATION	44
AU-11 AUDIT RECORD RETENTION	45
AU-12 AUDIT GENERATION	46
AU-13 MONITORING FOR INFORMATION DISCLOSURE	47
AU-14 SESSION AUDIT	48
AU-15 ALTERNATE AUDIT CAPABILITY	49
AU-16 CROSS-ORGANIZATIONAL AUDITING	50
AT - Awareness and Training Control Family	51
AT-1 SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES	52
AT-2 SECURITY AWARENESS TRAINING	53
AT-3 ROLE-BASED SECURITY TRAINING	54
AT-4 SECURITY TRAINING RECORDS	55

CM - Configuration Management Control Family	56
CM-1 CONFIGURATION MANAGEMENT POLICY AND PROCEDURES	57
CM-2 BASELINE CONFIGURATION	58
CM-3 CONFIGURATION CHANGE CONTROL	59
CM-4 SECURITY IMPACT ANALYSIS	60
CM-5 ACCESS RESTRICTIONS FOR CHANGE	61
CM-6 CONFIGURATION SETTINGS	62
CM-7 LEAST FUNCTIONALITY	63
CM-8 INFORMATION SYSTEM COMPONENT INVENTORY	64
CM-9 CONFIGURATION MANAGEMENT PLAN	65
CM-10 SOFTWARE USAGE RESTRICTIONS	66
CM-11 USER-INSTALLED SOFTWARE	67
CP - Contingency Planning Control Family	68
CP-1 CONTINGENCY PLANNING POLICY AND PROCEDURES	69
CP-2 CONTINGENCY PLAN	70
CP-3 CONTINGENCY TRAINING	72
CP-4 CONTINGENCY PLAN TESTING	73
CP-5 CONTINGENCY PLAN UPDATE	74
CP-6 ALTERNATE STORAGE SITE	75
CP-7 ALTERNATE PROCESSING SITE	76
CP-8 TELECOMMUNICATIONS SERVICES	77
CP-9 INFORMATION SYSTEM BACKUP	78
CP-10 INFORMATION SYSTEM RECOVERY AND RECONSTITUTION	79
CP-11 ALTERNATE COMMUNICATIONS PROTOCOLS	80
CP-12 SAFE MODE	81
CP-13 ALTERNATIVE SECURITY MECHANISMS	82
IA - Identification and Authentication Control Family	83
IA-1 IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES	84
IA-2 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)	85
IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION	86
IA-4 IDENTIFIER MANAGEMENT	87
IA-5 AUTHENTICATOR MANAGEMENT	88
IA-6 AUTHENTICATOR FEEDBACK	89
IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION	90
IA-8 IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)	91
IA-9 SERVICE IDENTIFICATION AND AUTHENTICATION	92
IA-10 ADAPTIVE IDENTIFICATION AND AUTHENTICATION	93
IA-11 RE-AUTHENTICATION	94
IR - Incident Response Control Family	95
IR-1 INCIDENT RESPONSE POLICY AND PROCEDURES	96
IR-2 INCIDENT RESPONSE TRAINING	97
IR-3 INCIDENT RESPONSE TESTING	98
IR-4 INCIDENT HANDLING	99
IR-5 INCIDENT MONITORING	100
IR-6 INCIDENT REPORTING	101
IR-7 INCIDENT RESPONSE ASSISTANCE	102
IR-8 INCIDENT RESPONSE PLAN	103
IR-9 INFORMATION SPILLAGE RESPONSE	104
IR-10 INTEGRATED INFORMATION SECURITY ANALYSIS TEAM	105
MA - Maintenance Control Family	106

MA-1 SYSTEM MAINTENANCE POLICY AND PROCEDURES	107
MA-2 CONTROLLED MAINTENANCE	108
MA-3 MAINTENANCE TOOLS	109
MA-4 NONLOCAL MAINTENANCE	110
MA-5 MAINTENANCE PERSONNEL	111
MA-6 TIMELY MAINTENANCE	112
MP - Media Protection Control Family	113
MP-1 MEDIA PROTECTION POLICY AND PROCEDURES	114
MP-2 MEDIA ACCESS	115
MP-3 MEDIA MARKING	116
MP-4 MEDIA STORAGE	117
MP-5 MEDIA TRANSPORT	118
MP-6 MEDIA SANITIZATION	119
MP-7 MEDIA USE	120
MP-8 MEDIA DOWNGRADING	121
Personnel Security Control Family	122
PS-1 PERSONNEL SECURITY POLICY AND PROCEDURES	123
PS-2 POSITION RISK DESIGNATION	124
PS-3 PERSONNEL SCREENING	125
PS-4 PERSONNEL TERMINATION	126
PS-5 PERSONNEL TRANSFER	127
PS-6 ACCESS AGREEMENTS	128
PS-7 THIRD-PARTY PERSONNEL SECURITY	129
PS-8 PERSONNEL SANCTIONS	130
PE - Physical and Environmental Protection Control Family	131
PE-1 PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES	
PE-2 PHYSICAL ACCESS AUTHORIZATIONS	133132
PE-3 PHYSICAL ACCESS CONTROL	134
PE-4 ACCESS CONTROL FOR TRANSMISSION MEDIUM	135
PE-5 ACCESS CONTROL FOR OUTPUT DEVICES	136
PE-6 MONITORING PHYSICAL ACCESS	137
PE-7 VISITOR CONTROL	138
PE-8 VISITOR ACCESS RECORDS	139
PE-9 POWER EQUIPMENT AND CABLING	140
PE-10 EMERGENCY SHUTOFF	141
PE-11 EMERGENCY POWER	142
PE-12 EMERGENCY LIGHTING	143
PE-13 FIRE PROTECTION	144
PE-14 TEMPERATURE AND HUMIDITY CONTROLS	145
PE-15 WATER DAMAGE PROTECTION	146
PE-16 DELIVERY AND REMOVAL	147
PE-17 ALTERNATE WORK SITE	148
PE-18 LOCATION OF INFORMATION SYSTEM COMPONENTS	149
PE-19 INFORMATION LEAKAGE	150
PE-20 ASSET MONITORING AND TRACKING	151
PL - Planning Control Family	152
PL-1 SECURITY PLANNING POLICY AND PROCEDURES	153
PL-2 SYSTEM SECURITY PLAN	154
PL-3 SYSTEM SECURITY PLAN UPDATE	156
PL-4 RULES OF BEHAVIOR	157

PL-5 PRIVACY IMPACT ASSESSMENT	158
PL-6 SECURITY-RELATED ACTIVITY PLANNING	159
PL-7 SECURITY CONCEPT OF OPERATIONS	160
PL-8 INFORMATION SECURITY ARCHITECTURE	161
PL-9 CENTRAL MANAGEMENT	162
Program Management Control Family	163
PM-1 INFORMATION SECURITY PROGRAM PLAN	164
PM-2 SENIOR INFORMATION SECURITY OFFICER	165
PM-3 INFORMATION SECURITY RESOURCES	166
PM-4 PLAN OF ACTION AND MILESTONES PROCESS	167
PM-5 INFORMATION SYSTEM INVENTORY	168
PM-6 INFORMATION SECURITY MEASURES OF PERFORMANCE	169
PM-7 ENTERPRISE ARCHITECTURE	170
PM-8 CRITICAL INFRASTRUCTURE PLAN	171
PM-9 RISK MANAGEMENT STRATEGY	172
PM-10 SECURITY AUTHORIZATION PROCESS	173
PM-11 MISSION/BUSINESS PROCESS DEFINITION	174
PM-12 INSIDER THREAT PROGRAM	175
PM-13 INFORMATION SECURITY WORKFORCE	176
PM-14 TESTING, TRAINING, AND MONITORING	177
PM-15 CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS	178
PM-16 THREAT AWARENESS PROGRAM	179
Risk Assessment Control Family	180
RA-1 RISK ASSESSMENT POLICY AND PROCEDURES	181
RA-2 SECURITY CATEGORIZATION	182
RA-3 RISK ASSESSMENT	183
RA-4 RISK ASSESSMENT UPDATE	184
RA-5 VULNERABILITY SCANNING	185
RA-6 TECHNICAL SURVEILLANCE COUNTERMEASURES SURVEY	186
CA - Security Assessment and Authorization Control Family	187
CA-1 SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES	
CA-2 SECURITY ASSESSMENTS	189188
CA-3 SYSTEM INTERCONNECTIONS	190
CA-5 PLAN OF ACTION AND MILESTONES	191
CA-6 SECURITY AUTHORIZATION	192
CA-7 CONTINUOUS MONITORING	193
CA-8 PENETRATION TESTING	194
CA-9 INTERNAL SYSTEM CONNECTIONS	195
System And Communications Protection Control Family	196
SC-1 SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES	
SC-2 APPLICATION PARTITIONING	199198
SC-3 SECURITY FUNCTION ISOLATION	200
SC-4 INFORMATION IN SHARED RESOURCES	201
SC-5 DENIAL OF SERVICE PROTECTION	202
SC-6 RESOURCE AVAILABILITY	203
SC-7 BOUNDARY PROTECTION	204
SC-8 TRANSMISSION CONFIDENTIALITY AND INTEGRITY	205
SC-9 TRANSMISSION CONFIDENTIALITY	206
SC-10 NETWORK DISCONNECT	207
SC-11 TRUSTED PATH	208

SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	209
SC-13 CRYPTOGRAPHIC PROTECTION	210
SC-14 PUBLIC ACCESS PROTECTIONS	211
SC-15 COLLABORATIVE COMPUTING DEVICES	212
SC-16 TRANSMISSION OF SECURITY ATTRIBUTES	213
SC-17 PUBLIC KEY INFRASTRUCTURE CERTIFICATES	214
SC-18 MOBILE CODE	215
SC-19 VOICE OVER INTERNET PROTOCOL	216
SC-20 SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)	217
SC-21 SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)	218
SC-22 ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE	219
SC-23 SESSION AUTHENTICITY	220
SC-24 FAIL IN KNOWN STATE	221
SC-25 THIN NODES	222
SC-26 HONEYPOTS	223
SC-27 PLATFORM-INDEPENDENT APPLICATIONS	224
SC-28 PROTECTION OF INFORMATION AT REST	225
SC-29 HETEROGENEITY	226
SC-30 CONCEALMENT AND MISDIRECTION	227
SC-31 COVERT CHANNEL ANALYSIS	228
SC-32 INFORMATION SYSTEM PARTITIONING	229
SC-33 TRANSMISSION PREPARATION INTEGRITY	230
SC-34 NON-MODIFIABLE EXECUTABLE PROGRAMS	231
SC-35 HONEYCLIENTS	232
SC-36 DISTRIBUTED PROCESSING AND STORAGE	233
SC-37 OUT-OF-BAND CHANNELS	234
SC-38 OPERATIONS SECURITY	235
SC-39 PROCESS ISOLATION	236
SC-40 WIRELESS LINK PROTECTION	237
SC-41 PORT AND I/O DEVICE ACCESS	238
SC-42 SENSOR CAPABILITY AND DATA	239
SC-43 USAGE RESTRICTIONS	240
SC-44 DETONATION CHAMBERS	241
System And Information Integrity Control Family	242
SI-1 SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES	243
SI-2 FLAW REMEDIATION	244
SI-3 MALICIOUS CODE PROTECTION	245
SI-4 INFORMATION SYSTEM MONITORING	246
SI-5 SECURITY ALERTS, ADVISORIES, AND DIRECTIVES	248
SI-6 SECURITY FUNCTION VERIFICATION	249
SI-7 SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY	250
SI-8 SPAM PROTECTION	251
SI-9 INFORMATION INPUT RESTRICTIONS	252
SI-10 INFORMATION INPUT VALIDATION	253
SI-11 ERROR HANDLING	254
SI-12 INFORMATION HANDLING AND RETENTION	255
SI-13 PREDICTABLE FAILURE PREVENTION	256

SI-14 NON-PERSISTENCE	257
SI-15 INFORMATION OUTPUT FILTERING	258
SI-16 MEMORY PROTECTION	259
SI-17 FAIL-SAFE PROCEDURES	260
System And Services Acquisition Control Family	261
SA-1 SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES	262
SA-2 ALLOCATION OF RESOURCES	263
SA-3 SYSTEM DEVELOPMENT LIFE CYCLE	264
SA-4 ACQUISITION PROCESS	265
SA-5 INFORMATION SYSTEM DOCUMENTATION	266
SA-6 SOFTWARE USAGE RESTRICTIONS	267
SA-7 USER-INSTALLED SOFTWARE	268
SA-8 SECURITY ENGINEERING PRINCIPLES	269
SA-9 EXTERNAL INFORMATION SYSTEM SERVICES	270
SA-10 DEVELOPER CONFIGURATION MANAGEMENT	271
SA-11 DEVELOPER SECURITY TESTING AND EVALUATION	272
SA-12 SUPPLY CHAIN PROTECTION	273
SA-13 TRUSTWORTHINESS	274
SA-14 CRITICALITY ANALYSIS	275
SA-15 DEVELOPMENT PROCESS, STANDARDS, AND TOOLS	276
SA-16 DEVELOPER-PROVIDED TRAINING	277
SA-17 DEVELOPER SECURITY ARCHITECTURE AND DESIGN	278
SA-18 TAMPER RESISTANCE AND DETECTION	279
SA-19 COMPONENT AUTHENTICITY	280
SA-20 CUSTOMIZED DEVELOPMENT OF CRITICAL COMPONENTS	281
SA-21 DEVELOPER SCREENING	282
SA-22 UNSUPPORTED SYSTEM COMPONENTS	283

Assessment of Pivotal Cloud Foundry against NIST SP 800-53(r4) Controls

Many organizations are required to reference a standardized control framework when assessing the security and compliance of their information systems. Standardized control frameworks are intended to provide a model for how to protect information and data systems from threats, including malicious third parties, structural failures, and human error. One very comprehensive and commonly referenced framework is NIST Special Publication 800-53(r4). Adherence to these controls is required for many government agencies in the United States, as well as for many private enterprises that operate within regulated markets, such as healthcare or finance. For example, the HIPAA regulations that govern the required protections for Personal Health Information (PHI) may be cross-referenced to the NIST SP 800-53(r4) control set.

These pages provide an assessment of the Pivotal Cloud Foundry PAS platform against the NIST SP 800-53(r4) controls, and provides guidance for how deployers may achieve compliance when using a shared responsibility model. Responsibility for any particular control may be assigned to the underlying IaaS infrastructure, the PAS platform, the deployed application, or the organization.

This document covers the Pivotal Cloud Foundry PAS, and assumes the use of BOSH and Ops Manager. In addition, we assume the platform has been deployed in a manner consistent with the corresponding IaaS reference architecture.

Control Families

- [AC - Access Control](#)
- [AU - Audit and Accountability](#)
- [AT - Awareness and Training](#)
- [CM - Configuration Management](#)
- [CP - Contingency Planning](#)
- [IA - Identification and Authentication](#)
- [IR - Incident Response](#)
- [MA - Maintenance](#)
- [MP - Media Protection](#)
- [PS - Personnel Security](#)
- [PE - Physical and Environmental Protection](#)
- [PL - Planning](#)
- [PM - Program Management](#)
- [RA - Risk Assessment](#)
- [CA - Security Assessment and Authorization](#)
- [SC - System and Communications Protection](#)
- [SI - System and Information Integrity](#)
- [SA - System and Services Acquisition](#)

AC - Access Control Control Family

Number	Control	Pivotal Application Service (PAS) Compliance
AC-1	ACCESS CONTROL POLICY AND PROCEDURES	Inherited and compliant
AC-2	ACCOUNT MANAGEMENT	Deployer Responsibility
AC-3	ACCESS ENFORCEMENT	Compliant
AC-4	INFORMATION FLOW ENFORCEMENT	Compliant
AC-5	SEPARATION OF DUTIES	Deployer Responsibility
AC-6	LEAST PRIVILEGE	Deployer Responsibility
AC-7	UNSUCCESSFUL LOGON ATTEMPTS	Inherited
AC-8	SYSTEM USE NOTIFICATION	Compliant
AC-9	PREVIOUS LOGON (ACCESS) NOTIFICATION	Inherited
AC-10	CONCURRENT SESSION CONTROL	Not required for FISMA moderate
AC-11	SESSION LOCK	Inherited
AC-12	SESSION TERMINATION	Compliant
AC-14	PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION	Compliant
AC-16	SECURITY ATTRIBUTES	P0, so not required for FISMA Moderate
AC-17	REMOTE ACCESS	Inherited and Compliant
AC-18	WIRELESS ACCESS	Compliant
AC-19	ACCESS CONTROL FOR MOBILE DEVICES	Not Applicable to PCF
AC-20	USE OF EXTERNAL INFORMATION SYSTEMS	Deployer Responsibility
AC-21	INFORMATION SHARING	Inherited and Compliant
AC-22	PUBLICLY ACCESSIBLE CONTENT	Inherited and Compliant
AC-23	DATA MINING PROTECTION	P0, so not required for FISMA Moderate
AC-24	ACCESS CONTROL DECISIONS	P0, so not required for FISMA Moderate
AC-25	REFERENCE MONITOR	P0, so not required for FISMA Moderate

AC-1 ACCESS CONTROL POLICY AND PROCEDURES

PCF Compliance

All requirements are the responsibility of the deployer. The PCF product feature set is sufficient to satisfy the technical requirements implied in AC-1. Pivotal may be able to provide guidance to customers who are creating or updating documentation, but this documentation is unique to the deployer's mission and business goals.

Control Description

The organization:

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

Supplemental Guidance

This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AC family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

AC-2 ACCOUNT MANAGEMENT

PCF Compliance

The PCF product feature set is sufficient to satisfy the technical requirements implied in AC-2. APIs are available to enable automation and reporting of account management. Policies and procedures that use these APIs are the responsibility of the deployer.

Control Description

The organization:

- a. Identifies and selects the following types of information system accounts to support organizational missions/business functions: [Assignment: organization-defined information system account types];
- b. Assigns account managers for information system accounts;
- c. Establishes conditions for group and role membership;
- d. 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;
- e. Requires approvals by [Assignment: organization-defined personnel or roles] for requests to create information system accounts;
- f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions];
- g. Monitors the use of information system accounts;
- h. 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;
- i. 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;
- j. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency]; and
- k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

Supplemental Guidance

Information system account types include, for example, individual, shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and service. Some of the account management requirements listed above can be implemented by organizational information systems. The identification of authorized users of the information system and the specification of access privileges reflects the requirements in other security controls in the security plan. Users requiring administrative privileges on information system accounts receive additional scrutiny by appropriate organizational personnel (e.g., system owner, mission/business owner, or chief information security officer) responsible for approving such accounts and privileged access. Organizations may choose to define access privileges or other attributes by account, by type of account, or a combination of both. Other attributes required for authorizing access include, for example, restrictions on time-of-day, day-of-week, and point-of-origin. In defining other account attributes, organizations consider system-related requirements (e.g., scheduled maintenance, system upgrades) and mission/business requirements, (e.g., time zone differences, customer requirements, remote access to support travel requirements). Failure to consider these factors could affect information system availability. Temporary and emergency accounts are accounts intended for short-term use. Organizations establish temporary accounts as a part of normal account activation procedures when there is a need for short-term accounts without the demand for

immediacy in account activation. Organizations establish emergency accounts in response to crisis situations and with the need for rapid account activation. Therefore, emergency account activation may bypass normal account authorization processes. Emergency and temporary accounts are not to be confused with infrequently used accounts (e.g., local logon accounts used for special tasks defined by organizations or when network resources are unavailable). Such accounts remain available and are not subject to automatic disabling or removal dates. Conditions for disabling or deactivating accounts include, for example: (i) when shared/group, emergency, or temporary accounts are no longer required; or (ii) when individuals are transferred or terminated. Some types of information system accounts may require specialized training.

AC-3 ACCESS ENFORCEMENT

PCF Compliance

The PCF product feature set is sufficient to satisfy the technical requirements implied in AC-3. PCF provides an [RBAC scheme](#) where roles are assigned to users and the users permission for any activities are scoped using the CAPI concepts of Orgs and Spaces. Enforcement of RBAC in the application is the responsibility of the application developers.

Control Description

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

Supplemental Guidance

Access control policies (e.g., identity-based policies, role-based policies, control matrices, cryptography) control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (e.g., devices, files, records, domains) in information systems. In addition to enforcing authorized access at the information system level and recognizing that information systems can host many applications and services in support of organizational missions and business operations, access enforcement mechanisms can also be employed at the application and service level to provide increased information security.

AC-4 INFORMATION FLOW ENFORCEMENT

PCF Compliance

The PCF product feature set is sufficient to satisfy the technical requirements implied in AC-4. PCF provides ingress controls through the CF router and route services. PCF provides egress control through Application Security Groups (ASGs). PCF provides intra-platform flow control through C2C networking policies.

Control Description

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].

Supplemental Guidance

Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. Flow control restrictions include, for example, keeping export-controlled information from being transmitted in the clear to the Internet, blocking outside traffic that claims to be from within the organization, restricting web requests to the Internet that are not from the internal web proxy server, and limiting information transfers between organizations based on data structures and content. Transferring information between information systems representing different security domains with different security policies introduces risk that such transfers violate one or more domain security policies. In such situations, information owners/stewards provide guidance at designated policy enforcement points between interconnected systems. Organizations consider mandating specific architectural solutions when required to enforce specific security policies. Enforcement includes, for example: (i) prohibiting information transfers between interconnected systems (i.e., allowing access only); (ii) employing hardware mechanisms to enforce one-way information flows; and (iii) implementing trustworthy regrading mechanisms to reassign security attributes and security labels. Organizations commonly employ information flow control policies and enforcement mechanisms to control the flow of information between designated sources and destinations (e.g., networks, individuals, and devices) within information systems and between interconnected systems. Flow control is based on the characteristics of the information and/or the information path. Enforcement occurs, for example, in boundary protection devices (e.g., gateways, routers, guards, encrypted tunnels, firewalls) that employ rule sets or establish configuration settings that restrict information system services, provide a packet-filtering capability based on header information, or message-filtering capability based on message content (e.g., implementing key word searches or using document characteristics). Organizations also consider the trustworthiness of filtering/inspection mechanisms (i.e., hardware, firmware, and software components) that are critical to information flow enforcement. Control enhancements 3 through 22 primarily address cross-domain solution needs which focus on more advanced filtering techniques, in-depth analysis, and stronger flow enforcement mechanisms implemented in cross-domain products, for example, high-assurance guards. Such capabilities are generally not available in commercial off-the-shelf information technology products.

AC-5 SEPARATION OF DUTIES

PCF Compliance

PCF provides basic [RBAC support](#). Enforcement of separation of duties (SOD) is the responsibility of the deployer.

PCF supports assignment of specific roles so that users may be given separate duties as appropriate. Granularity of permission set in a defined role is fixed. Additional controls may be inherited from systems external to PCF.

Control Description

The organization:

- a. Separates [Assignment: organization-defined duties of individuals];
- b. Documents separation of duties of individuals; and
- c. Defines information system access authorizations to support separation of duties.

Supplemental Guidance

Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes, for example: (i) dividing mission functions and information system support functions among different individuals and/or roles; (ii) conducting information system support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, and network security); and (iii) ensuring security personnel administering access control functions do not also administer audit functions.

AC-6 LEAST PRIVILEGE

PCF Compliance

PCF provides basic [RBAC support](#). Enforcement of separation of duties (SOD) is the responsibility of the deployer.

PCF supports assignment of specific roles so that users may be given separate duties as appropriate. Granularity of permission set in a defined role is fixed. Additional controls may be inherited from systems external to PCF.

Control Description

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.

Supplemental Guidance

Organizations employ least privilege for specific duties and information systems. The principle of least privilege is also applied to information system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions/business functions. Organizations consider the creation of additional processes, roles, and information system accounts as necessary, to achieve least privilege. Organizations also apply least privilege to the development, implementation, and operation of organizational information systems.

AC-7 UNSUCCESSFUL LOGON ATTEMPTS

PCF Compliance

In PCF, the UAA component delegates these responsibilities to the enterprise identity management system (IdM). Lockout of users following too many failed authentication attempts is inherited from the enterprise IdM. In the case of BOSH SSH, users must have previously authenticated via UAA, and the SSH login uses a BOSH-managed private key.

Control Description

The information system:

- a. Enforces a limit of [Assignment: organization-defined number] consecutive invalid logon attempts by a user during a [Assignment: organization-defined time period]; and
- b. Automatically [Selection: locks the account/node for an [Assignment: organization-defined time period]; 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.

Supplemental Guidance

This control applies regardless of whether the logon occurs via a local or network connection. Due to the potential for denial of service, automatic lockouts initiated by information systems are usually temporary and automatically release after a predetermined time period established by organizations. If a delay algorithm is selected, organizations may choose to employ different algorithms for different information system components based on the capabilities of those components. Responses to unsuccessful logon attempts may be implemented at both the operating system and the application levels.

AC-8 SYSTEM USE NOTIFICATION

PCF Compliance

PCF is compliant with this requirement. PCF provides a feature that allows the deployer to configure an organization-defined system use notification message or banner in the Ops Manager and Apps Manager UIs. Similarly, configuration of a site-specific banner during SSH sessions into stemcells is available using BOSH Add-on.

Control Description

The organization:

- a. Displays to users [Assignment: organization-defined system use notification message or banner] 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;
- b. 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
- c. For publicly accessible systems:
 1. Displays system use information [Assignment: organization-defined conditions], 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.


Supplemental Guidance

System use notifications can be implemented using messages or warning banners displayed before individuals log in to information systems. System use notifications are used only for access via logon interfaces with human users and are not required when such human interfaces do not exist. Organizations consider system use notification messages/banners displayed in multiple languages based on specific organizational needs and the demographics of information system users. Organizations also consult with the Office of the General Counsel for legal review and approval of warning banner content.

AC-9 PREVIOUS LOGON (ACCESS) NOTIFICATION

PCF Compliance

This control is inherited by PCF. All identity management function, such as notification of a previous log in event, are delegated to the enterprise identity management system.

 **Note:** This control is P0 priority and not required for FISMA moderate.

Control Description

The information system notifies the user, upon successful logon (access) to the system, of the date and time of the last logon (access).

Supplemental Guidance

This control is applicable to logons to information systems via human user interfaces and logons to systems that occur in other types of architectures (e.g., service-oriented architectures).

AC-10 CONCURRENT SESSION CONTROL

PCF Compliance

This control is not required for [FISMA](#) Moderate.

Control Description

The information system limits the number of concurrent sessions for each [Assignment: organization-defined account and/or account type] to [Assignment: organization-defined number].

Supplemental Guidance


Organizations may define the maximum number of concurrent sessions for information system accounts globally, by account type (e.g., privileged user, non-privileged user, domain, specific application), by account, or a combination. For example, organizations may limit the number of concurrent sessions for system administrators or individuals working in particularly sensitive domains or mission-critical applications. This control addresses concurrent sessions for information system accounts and does not address concurrent sessions by single users via multiple system accounts.

AC-11 SESSION LOCK

PCF Compliance

This control is inherited from the client desktop. All desktop, laptop, and tablet clients have a screen lock provided. Enforcing the use of this session lock at the client device is the responsibility of the deployer.

PCF uses OAuth 2 tokens with session timeout, but does not maintain locked sessions.

 **Note:** This control is P3, which is a lower level of priority for the compliant organization

Control Description

The information system:

- a. Prevents further access to the system by initiating a session lock after [Assignment: organization-defined time period] of inactivity or upon receiving a request from a user; and
- b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.

Supplemental Guidance

Session locks are temporary actions taken when users stop work and move away from the immediate vicinity of information systems but do not want to log out because of the temporary nature of their absences. Session locks are implemented where session activities can be determined. This is typically at the operating system level, but can also be at the application level. Session locks are not an acceptable substitute for logging out of information systems, for example, if organizations require users to log out at the end of workdays.

AC-12 SESSION TERMINATION

PCF Compliance

PCF is compliant with this requirement through configuration of UAA token timeout. Additionally, compliance is supported for BOSH SSH sessions through configuration of stemcell through BOSH Add-on.

Control Description

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

Supplemental Guidance

This control addresses the termination of user-initiated logical sessions in contrast to SC-10 which addresses the termination of network connections that are associated with communications sessions (i.e., network disconnect). A logical session (for local, network, and remote access) is initiated whenever a user (or process acting on behalf of a user) accesses an organizational information system. Such user sessions can be terminated (and thus terminate user access) without terminating network sessions. Session termination terminates all processes associated with a user's logical session except those processes that are specifically created by the user (i.e., session owner) to continue after the session is terminated. Conditions or trigger events requiring automatic session termination can include, for example, organization-defined periods of user inactivity, targeted responses to certain types of incidents, time-of-day restrictions on information system use.

AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION

PCF Compliance

PCF is compliant with this requirement. Any actions that affect the state of the PCF installation require users to log in. Applications running on PCF, however, may choose to offer pages with no authentication, if and as appropriate.

Control Description

The organization:

- a. 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
- b. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification or authentication.

Supplemental Guidance

This control addresses situations in which organizations determine that no identification or authentication is required in organizational information systems. Organizations may allow a limited number of user actions without identification or authentication including, for example, when individuals access public websites or other publicly accessible federal information systems, when individuals use mobile phones to receive calls, or when facsimiles are received. Organizations also identify actions that normally require identification or authentication but may under certain circumstances (e.g., emergencies), allow identification or authentication mechanisms to be bypassed. Such bypasses may occur, for example, via a software-readable physical switch that commands bypass of the logon functionality and is protected from accidental or unmonitored use. This control does not apply to situations where identification and authentication have already occurred and are not repeated, but rather to situations where identification and authentication have not yet occurred. Organizations may decide that there are no user actions that can be performed on organizational information systems without identification and authentication and thus, the values for assignment statements can be none.

AC-16 SECURITY ATTRIBUTES

PCF Compliance

This control is P0 priority and not required for [FISMA](#) Moderate.

Control Description

The organization:

- a. Provides the means to associate [Assignment: organization-defined types of security attributes] having [Assignment: organization-defined security attribute values] with information in storage, in process, and/or in transmission;
- b. Ensures that the security attribute associations are made and retained with the information;
- c. Establishes the permitted [Assignment: organization-defined security attributes] for [Assignment: organization-defined information systems]; and
- d. Determines the permitted [Assignment: organization-defined values or ranges] for each of the established security attributes.

Supplemental Guidance

Information is represented internally within information systems using abstractions known as data structures. Internal data structures can represent different types of entities, both active and passive. Active entities, also known as subjects, are typically associated with individuals, devices, or processes acting on behalf of individuals. Passive entities, also known as objects, are typically associated with data structures such as records, buffers, tables, files, inter-process pipes, and communications ports. Security attributes, a form of metadata, are abstractions representing the basic properties or characteristics of active and passive entities with respect to safeguarding information. These attributes may be associated with active entities (i.e., subjects) that have the potential to send or receive information, to cause information to flow among objects, or to change the information system state. These attributes may also be associated with passive entities (i.e., objects) that contain or receive information. The association of security attributes to subjects and objects is referred to as binding and is typically inclusive of setting the attribute value and the attribute type. Security attributes when bound to data/information, enables the enforcement of information security policies for access control and information flow control, either through organizational processes or information system functions or mechanisms. The content or assigned values of security attributes can directly affect the ability of individuals to access organizational information. Organizations can define the types of attributes needed for selected information systems to support missions/business functions. There is potentially a wide range of values that can be assigned to any given security attribute. Release markings could include, for example, US only, NATO, or NOFORN (not releasable to foreign nationals). By specifying permitted attribute ranges and values, organizations can ensure that the security attribute values are meaningful and relevant. The term security labeling refers to the association of security attributes with subjects and objects represented by internal data structures within organizational information systems, to enable information system-based enforcement of information security policies. Security labels include, for example, access authorizations, data life cycle protection (i.e., encryption and data expiration), nationality, affiliation as contractor, and classification of information in accordance with legal and compliance requirements. The term security marking refers to the association of security attributes with objects in a human-readable form, to enable organizational process-based enforcement of information security policies. The AC-16 base control represents the requirement for user-based attribute association (marking). The enhancements to AC-16 represent additional requirements including information system-based attribute association (labeling). Types of attributes include, for example, classification level for objects and clearance (access authorization) level for subjects. An example of a value for both of these attribute types is Top Secret.

AC-17 REMOTE ACCESS

PCF Compliance

PCF complies with this requirement by providing TLS 1.2 support for all user network connections. However, PCF does not provide any native support for “remote” access, and inherits controls from the supporting infrastructure.

Control Description

The organization:

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

Supplemental Guidance

Remote access is access to organizational information systems by users (or processes acting on behalf of users) communicating through external networks (e.g., the Internet). Remote access methods include, for example, dial-up, broadband, and wireless. Organizations often employ encrypted virtual private networks (VPNs) to enhance confidentiality and integrity over remote connections. The use of encrypted VPNs does not make the access non-remote; however, the use of VPNs, when adequately provisioned with appropriate security controls (e.g., employing appropriate encryption techniques for confidentiality and integrity protection) may provide sufficient assurance to the organization that it can effectively treat such connections as internal networks. Still, VPN connections traverse external networks, and the encrypted VPN does not enhance the availability of remote connections. Also, VPNs with encrypted tunnels can affect the organizational capability to adequately monitor network communications traffic for malicious code. Remote access controls apply to information systems other than public web servers or systems designed for public access. This control addresses authorization prior to allowing remote access without specifying the formats for such authorization. While organizations may use interconnection security agreements to authorize remote access connections, such agreements are not required by this control. Enforcing access restrictions for remote connections is addressed in AC-3.

AC-18 WIRELESS ACCESS

PCF Compliance

Compliance with this requirement is the responsibility of the deployer. A PCF installation leverages network resources provided by the IaaS layer, therefore compliance with this requirement is inherited based upon the deployer's choice of network technologies.

Control Description

The organization:

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

Supplemental Guidance

Wireless technologies include, for example, microwave, packet radio (UHF/VHF), 802.11x, and Bluetooth. Wireless networks use authentication protocols (e.g., EAP/TLS, PEAP), which provide credential protection and mutual authentication.

AC-19 ACCESS CONTROL FOR MOBILE DEVICES

PCF Compliance

This control is not applicable to PCF.

Control Description

The organization:

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

Supplemental Guidance

A mobile device is a computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable or removable data storage; and (iv) includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the device to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, E-readers, and tablets. Mobile devices are typically associated with a single individual and the device is usually in close proximity to the individual; however, the degree of proximity can vary depending upon on the form factor and size of the device. The processing, storage, and transmission capability of the mobile device may be comparable to or merely a subset of desktop systems, depending upon the nature and intended purpose of the device. Due to the large variety of mobile devices with different technical characteristics and capabilities, organizational restrictions may vary for the different classes/types of such devices. Usage restrictions and specific implementation guidance for mobile devices include, for example, configuration management, device identification and authentication, implementation of mandatory protective software (e.g., malicious code detection, firewall), scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless, infrared). Organizations are cautioned that the need to provide adequate security for mobile devices goes beyond the requirements in this control. Many safeguards and countermeasures for mobile devices are reflected in other security controls in the catalog allocated in the initial control baselines as starting points for the development of security plans and overlays using the tailoring process. There may also be some degree of overlap in the requirements articulated by the security controls within the different families of controls. AC-20 addresses mobile devices that are not organization-controlled.

AC-20 USE OF EXTERNAL INFORMATION SYSTEMS

PCF Compliance

This control is out of scope for PCF. Compliance is the responsibility of the PCF deployer.

Control Description

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:

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

Supplemental Guidance

External information systems are information systems or components of information systems that are outside of the authorization boundary established by organizations and for which organizations typically have no direct supervision and authority over the application of required security controls or the assessment of control effectiveness. External information systems include, for example: (i) personally owned information systems/devices (e.g., notebook computers, smart phones, tablets, personal digital assistants); (ii) privately owned computing and communications devices resident in commercial or public facilities (e.g., hotels, train stations, convention centers, shopping malls, or airports); (iii) information systems owned or controlled by nonfederal governmental organizations; and (iv) federal information systems that are not owned by, operated by, or under the direct supervision and authority of organizations. This control also addresses the use of external information systems for the processing, storage, or transmission of organizational information, including, for example, accessing cloud services (e.g., infrastructure as a service, platform as a service, or software as a service) from organizational information systems. For some external information systems (i.e., information systems operated by other federal agencies, including organizations subordinate to those agencies), the trust relationships that have been established between those organizations and the originating organization may be such, that no explicit terms and conditions are required. Information systems within these organizations would not be considered external. These situations occur when, for example, there are pre-existing sharing/trust agreements (either implicit or explicit) established between federal agencies or organizations subordinate to those agencies, or when such trust agreements are specified by applicable laws, Executive Orders, directives, or policies. Authorized individuals include, for example, organizational personnel, contractors, or other individuals with authorized access to organizational information systems and over which organizations have the authority to impose rules of behavior with regard to system access. Restrictions that organizations impose on authorized individuals need not be uniform, as those restrictions may vary depending upon the trust relationships between organizations. Therefore, organizations may choose to impose different security restrictions on contractors than on state, local, or tribal governments. This control does not apply to the use of external information systems to access public interfaces to organizational information systems (e.g., individuals accessing federal information through www.usa.gov). Organizations establish terms and conditions for the use of external information systems in accordance with organizational security policies and procedures. Terms and conditions address as a minimum: types of applications that can be accessed on organizational information systems from external information systems; and the highest security category of information that can be processed, stored, or transmitted on external information systems. If terms and conditions with the owners of external information systems cannot be established, organizations may impose restrictions on organizational personnel using those external systems.

AC-21 INFORMATION SHARING

PCF Compliance

PCF enables compliance with this requirement by providing SAMLv2 support. An organization can implement appropriate federation using available protocols and APIs if and as needed. Information sharing by an application is the responsibility of the application deployer.

Control Description

The organization:

- a. 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
- b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions.

Supplemental Guidance

This control applies to information that may be restricted in some manner (e.g., privileged medical information, contract-sensitive information, proprietary information, personally identifiable information, classified information related to special access programs or compartments) based on some formal or administrative determination. Depending on the particular information-sharing circumstances, sharing partners may be defined at the individual, group, or organizational level. Information may be defined by content, type, security category, or special access program/compartment.

AC-22 PUBLICLY ACCESSIBLE CONTENT

PCF Compliance

PCF provides logical access control for developers and operators through orgs and spaces. These features may be used to satisfy this requirement within PCF. Access control rules for maintenance of user generated content is the responsibility of the application deployer, and would be an inherited control.

Control Description

The organization:

- a. Designates individuals authorized to post information onto a publicly accessible information system;
- b. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information;
- c. Reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included; and
- d. Reviews the content on the publicly accessible information system for nonpublic information [Assignment: organization-defined frequency] and removes such information, if discovered.

Supplemental Guidance

In accordance with federal laws, Executive Orders, directives, policies, regulations, standards, and/or guidance, the general public is not authorized access to nonpublic information (e.g., information protected under the Privacy Act and proprietary information). This control addresses information systems that are controlled by the organization and accessible to the general public, typically without identification or authentication. The posting of information on non-organization information systems is covered by organizational policy.

AC-23 DATA MINING PROTECTION

PCF Compliance

This control is P0 priority and not required for [FISMA](#) Moderate.

Control Description

The organization employs [Assignment: organization-defined data mining prevention and detection techniques] for [Assignment: organization-defined data storage objects] to adequately detect and protect against data mining.

Supplemental Guidance

Data storage objects include, for example, databases, database records, and database fields. Data mining prevention and detection techniques include, for example: (i) limiting the types of responses provided to database queries; (ii) limiting the number/frequency of database queries to increase the work factor needed to determine the contents of such databases; and (iii) notifying organizational personnel when atypical database queries or accesses occur. This control focuses on the protection of organizational information from data mining while such information resides in organizational data stores. In contrast, AU-13 focuses on monitoring for organizational information that may have been mined or otherwise obtained from data stores and is now available as open source information residing on external sites, for example, through social networking or social media websites.

AC-24 ACCESS CONTROL DECISIONS

PCF Compliance

This control is P0 priority and not required for [FISMA](#) Moderate.

Control Description

The organization establishes procedures to ensure [Assignment: organization-defined access control decisions] are applied to each access request prior to access enforcement.

Supplemental Guidance

Access control decisions (also known as authorization decisions) occur when authorization information is applied to specific accesses. In contrast, access enforcement occurs when information systems enforce access control decisions. While it is very common to have access control decisions and access enforcement implemented by the same entity, it is not required and it is not always an optimal implementation choice. For some architectures and distributed information systems, different entities may perform access control decisions and access enforcement.

AC-25 REFERENCE MONITOR

PCF Compliance

This control is P0 priority and not required for [FISMA](#) Moderate.

Control Description

The information system implements a reference monitor for [Assignment: organization-defined access control policies] that is tamperproof, always invoked, and small enough to be subject to analysis and testing, the completeness of which can be assured.

Supplemental Guidance

Information is represented internally within information systems using abstractions known as data structures. Internal data structures can represent different types of entities, both active and passive. Active entities, also known as subjects, are typically associated with individuals, devices, or processes acting on behalf of individuals. Passive entities, also known as objects, are typically associated with data structures such as records, buffers, tables, files, inter-process pipes, and communications ports. Reference monitors typically enforce mandatory access control policies – a type of access control that restricts access to objects based on the identity of subjects or groups to which the subjects belong. The access controls are mandatory because subjects with certain privileges (i.e., access permissions) are restricted from passing those privileges on to any other subjects, either directly or indirectly – that is, the information system strictly enforces the access control policy based on the rule set established by the policy. The tamperproof property of the reference monitor prevents adversaries from compromising the functioning of the mechanism. The always invoked property prevents adversaries from bypassing the mechanism and hence violating the security policy. The smallness property helps to ensure the completeness in the analysis and testing of the mechanism to detect weaknesses or deficiencies (i.e., latent flaws) that would prevent the enforcement of the security policy.

AU - Audit and Accountability Control Family

Number	Control	Pivotal Application Service (PAS) Compliance
AU-1	AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES	Deployer Responsibility
AU-2	AUDIT EVENTS	Inherited and Compliant
AU-3	CONTENT OF AUDIT RECORDS	Compliant
AU-4	AUDIT STORAGE CAPACITY	Inherited
AU-5	RESPONSE TO AUDIT PROCESSING FAILURES	Compliant
AU-6	AUDIT REVIEW, ANALYSIS, AND REPORTING	deployer responsibility
AU-7	AUDIT REDUCTION AND REPORT GENERATION	Inherited
AU-8	TIME STAMPS	Compliant
AU-9	PROTECTION OF AUDIT INFORMATION	Inherited
AU-10	NON-REPUDIATION	Not required for FISMA moderate
AU-11	AUDIT RECORD RETENTION	Inherited
AU-12	AUDIT GENERATION	Inherited and Compliant
AU-13	MONITORING FOR INFORMATION DISCLOSURE	P0, so not required for FISMA Moderate
AU-14	SESSION AUDIT	P0, so not required for FISMA Moderate
AU-15	ALTERNATE AUDIT CAPABILITY	P0, so not required for FISMA Moderate
AU-16	CROSS-ORGANIZATIONAL AUDITING	P0, so not required for FISMA Moderate

AU-1 AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES

PCF Compliance

All requirements are the responsibility of the deployer. The PCF product feature set is sufficient to satisfy the technical requirements implied in AU-1. Pivotal may be able to provide guidance to customers who are creating or updating documentation, but this documentation is unique to the deployer's mission and business goals.

Control Description

The organization:

- a. 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
- b. Reviews and updates the current:
 1. Audit and accountability policy [Assignment: organization-defined frequency]; and
 2. Audit and accountability procedures [Assignment: organization-defined frequency].

Supplemental Guidance

This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AU family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

AU-2 AUDIT EVENTS

PCF Compliance

Policies and procedures are the responsibility of the deployer. All significant state transition events for the PCF platform are recorded in the logs. Any activity from the Cloud Controller API and the UAA are audited and available via syslog. In addition, logs from BOSH director and the Ops Manager VM are also sent to syslog. Contents of application audit logs are the responsibility of the deployer. The operator must configure a syslog destination at deployment time.

Control Description

The organization:

- a. Determines that the information system is capable of auditing the following events: [Assignment: organization-defined auditable events];
- b. 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;
- c. Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and
- d. Determines that the following events are to be audited within the information system: [Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a.) along with the frequency of (or situation requiring) auditing for each identified event].

Supplemental Guidance

An event is any observable occurrence in an organizational information system. Organizations identify audit events as those events which are significant and relevant to the security of information systems and the environments in which those systems operate in order to meet specific and ongoing audit needs. Audit events can include, for example, password changes, failed logons, or failed accesses related to information systems, administrative privilege usage, PIV credential usage, or third-party credential usage. In determining the set of auditable events, organizations consider the auditing appropriate for each of the security controls to be implemented. To balance auditing requirements with other information system needs, this control also requires identifying that subset of auditable events that are audited at a given point in time. For example, organizations may determine that information systems must have the capability to log every file access both successful and unsuccessful, but not activate that capability except for specific circumstances due to the potential burden on system performance. Auditing requirements, including the need for auditable events, may be referenced in other security controls and control enhancements. Organizations also include auditable events that are required by applicable federal laws, Executive Orders, directives, policies, regulations, and standards. Audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the appropriate level of abstraction is a critical aspect of an audit capability and can facilitate the identification of root causes to problems. Organizations consider in the definition of auditable events, the auditing necessary to cover related events such as the steps in distributed, transaction-based processes (e.g., processes that are distributed across multiple organizations) and actions that occur in service-oriented architectures.

AU-3 CONTENT OF AUDIT RECORDS

PCF Compliance

Content of audit log stream includes all appropriate context to enable a reviewer to determine who did what, how, and when. The log stream includes audit log information from 3 sources: PCF platform job logs, Linux OS audit logs, and application logs.

Control Description

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.

Supplemental Guidance

Audit record content that may be necessary to satisfy the requirement of this control, includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked. Event outcomes can include indicators of event success or failure and event-specific results (e.g., the security state of the information system after the event occurred).

AU-4 AUDIT STORAGE CAPACITY

PCF Compliance

Provisioning adequate audit log storage capacity is the responsibility of the deployer and operator. The PCF Loggregator system will forward all platform and application logs to an operator configured enterprise log management system. All audit logs are streamed off the platform as they are created, and forwarded to the syslog endpoint. Ops Manager and BOSH enable operators to adjust resource allocations for PCF VM capacity as needed.

Control Description

The organization allocates audit record storage capacity in accordance with [Assignment: organization-defined audit record storage requirements].

Supplemental Guidance

Organizations consider the types of auditing to be performed and the audit processing requirements when allocating audit storage capacity. Allocating sufficient audit storage capacity reduces the likelihood of such capacity being exceeded and resulting in the potential loss or reduction of auditing capability.

AU-5 RESPONSE TO AUDIT PROCESSING FAILURES

PCF Compliance

PCF delegates responsibility for audit logging alerts to the existing enterprise log management system. When appropriately configured, PCF will forward all activity logging to the designated enterprise log management system, and alerts or triggers for specific events may be established there. All implied requirements for this requirement are satisfied by the PCF platform.

Control Description

The organization:

- a. Alerts [Assignment: organization-defined personnel or roles] in the event of an audit processing failure; and
- b. Takes the following additional actions: [Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)].

Supplemental Guidance

Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded. Organizations may choose to define additional actions for different audit processing failures (e.g., by type, by location, by severity, or a combination of such factors). This control applies to each audit data storage repository (i.e., distinct information system component where audit records are stored), the total audit storage capacity of organizations (i.e., all audit data storage repositories combined), or both.

AU-6 AUDIT REVIEW, ANALYSIS, AND REPORTING

PCF Compliance

Compliance with this requirement is the deployer's responsibility. The organization must define appropriate policies, and implement the supplementary procedural controls. All implied technical requirements are satisfied by the PCF platform.

Details

policy and procedure

Control Description

The organization:

- a. Reviews and analyzes information system audit records [Assignment: organization-defined frequency] for indications of [Assignment: organization-defined inappropriate or unusual activity]; and
- b. Reports findings to [Assignment: organization-defined personnel or roles].

Supplemental Guidance

Audit review, analysis, and reporting covers information security-related auditing performed by organizations including, for example, auditing that results from monitoring of account usage, remote access, wireless connectivity, mobile device connection, configuration settings, system component inventory, use of maintenance tools and nonlocal maintenance, physical access, temperature and humidity, equipment delivery and removal, communications at the information system boundaries, use of mobile code, and use of VoIP. Findings can be reported to organizational entities that include, for example, incident response team, help desk, information security group/department. If organizations are prohibited from reviewing and analyzing audit information or unable to conduct such activities (e.g., in certain national security applications or systems), the review/analysis may be carried out by other organizations granted such authority.

AU-7 AUDIT REDUCTION AND REPORT GENERATION

PCF Compliance

Compliance with this requirement is a deployer responsibility. All implied technical control requirements are satisfied by the PCF platform. PCF provides comprehensive audit logging for all platform activity, which can be integrated with an enterprise log management system. Audit logging includes BOSH and Ops Manager actions, Cloud Controller and UAA actions, Linux OS auditing and application logging. In addition, these components of PCF also provide APIs to enable development of any custom reports required.

Control Description

The information system provides an audit reduction and report generation capability that:

- a. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and
- b. Does not alter the original content or time ordering of audit records.

Supplemental Guidance

Audit reduction is a process that manipulates collected audit information and organizes such information in a summary format that is more meaningful to analysts. Audit reduction and report generation capabilities do not always emanate from the same information system or from the same organizational entities conducting auditing activities. Audit reduction capability can include, for example, modern data mining techniques with advanced data filters to identify anomalous behavior in audit records. The report generation capability provided by the information system can generate customizable reports. Time ordering of audit records can be a significant issue if the granularity of the timestamp in the record is insufficient.

AU-8 TIME STAMPS

PCF Compliance

PCF is compliant with this requirement. The PCF deployment may be configured to use an NTP time server. All VM instances created by BOSH use an NTP client cron job to synchronize time across the machines in the deployment. The PCF deployment includes a “Clock Global” job and deployers may scale the number of instances as needed.

Control Description

The information system:

- a. Uses internal system clocks to generate time stamps for audit records; and
- b. 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].

Supplemental Guidance

Time stamps generated by the information system include date and time. Time is commonly expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC. Granularity of time measurements refers to the degree of synchronization between information system clocks and reference clocks, for example, clocks synchronizing within hundreds of milliseconds or within tens of milliseconds. Organizations may define different time granularities for different system components. Time service can also be critical to other security capabilities such as access control and identification and authentication, depending on the nature of the mechanisms used to support those capabilities.

AU-9 PROTECTION OF AUDIT INFORMATION

PCF Compliance

PCF satisfies all of the implied technical control requirements. The organization's procedural controls will be inherited by the PCF deployment. PCF may be configured to protect audit data using TLS as it is transferred from the PCF environment to the enterprise log management system. PCF provides native controls for limiting access to application logs while these logs are present within the PCF environment, via Cloud Controller logical access controls including RBAC roles, and the appropriate use of Orgs and Spaces by the deployer.

Deployers that require immutability of the Linux OS audit log rules must create a BOSH Add-on release.

The default configuration of the stemcell does not mark the Linux audit rules file as immutable because this would block the deployer from appending additional audit rules when deploying, for example, a site-specific security agent.

Once audit log data has been transferred to the enterprise log management system, the protection of archived audit log information from unauthorized access, modification, and deletion is the responsibility of the deployer.

Details

Control Description

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

Supplemental Guidance

Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity. This control focuses on technical protection of audit information. Physical protection of audit information is addressed by media protection controls and physical and environmental protection controls.

AU-10 NON-REPUDIATION

PCF Compliance

Audit log integrity is supported through logical access controls within the PAS itself, and via the controls in the underlying cloud infrastructure. Within the PCF platform, there are no native provisions to support cryptographic non-repudiation of audit log records using, for example, a digital signature. However, this non-repudiation control will be inherited by PCF when it is provided by the enterprise log management system. This control is not required for compliance for [FISMA](#) Moderate.

Control Description

The information system protects against an individual (or process acting on behalf of an individual) falsely denying having performed [Assignment: organization-defined actions to be covered by non-repudiation].

Supplemental Guidance

Types of individual actions covered by non-repudiation include, for example, creating information, sending and receiving messages, approving information (e.g., indicating concurrence or signing a contract). Non-repudiation protects individuals against later claims by: (i) authors of not having authored particular documents; (ii) senders of not having transmitted messages; (iii) receivers of not having received messages; or (iv) signatories of not having signed documents. Non-repudiation services can be used to determine if information originated from a particular individual, or if an individual took specific actions (e.g., sending an email, signing a contract, approving a procurement request) or received specific information. Organizations obtain non-repudiation services by employing various techniques or mechanisms (e.g., digital signatures, digital message receipts).

AU-11 AUDIT RECORD RETENTION

PCF Compliance

Compliance with this requirement is primarily a deployer responsibility. All implied technical control requirements are satisfied by the PCF platform. Definition of an appropriate retention policy, and the associated procedural controls, are the responsibility of the deployer. The PCF platform simply inherits the operational controls that have been defined by the organization.

Control Description

The organization retains audit records for [Assignment: organization-defined time period consistent with records retention policy] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

Supplemental Guidance

Organizations retain audit records until it is determined that they are no longer needed for administrative, legal, audit, or other operational purposes. This includes, for example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoenas, and law enforcement actions. Organizations develop standard categories of audit records relative to such types of actions and standard response processes for each type of action. The National Archives and Records Administration (NARA) General Records Schedules provide federal policy on record retention.

AU-12 AUDIT GENERATION

PCF Compliance

The policy decision on what events to audit is a deployer responsibility. However, all technical controls implied by this requirement are satisfied by the PCF platform.

When appropriately configured, the PCF platform audits all platform activity, and is compliant with this requirement.

It is the responsibility of the deployer to configure an appropriate syslog destination, and also to leverage appropriate encryption and logical access controls for all audit data that is archived off-platform to an enterprise log management system.

PCF platform and application logs are synchronized to an enterprise provided time standard, and thus may be correlated with logs from other information systems as needed. The logging format for Cloud Controller and UAA follows the de-facto standard CEF logging format.

Additional information on specific audit capabilities can be found on the following pages:

- [Logging Configuration](#)
- [Cloud Controller and UAA Logging](#)
- [BOSH Director Logging](#)

Control Description

The information system:

- Provides audit record generation capability for the auditable events defined in AU-2 a. at [Assignment: organization-defined information system components];
- Allows [Assignment: organization-defined personnel or roles] to select which auditable events are to be audited by specific components of the information system; and
- Generates audit records for the events defined in AU-2 d. with the content defined in AU-3.

Supplemental Guidance

Audit records can be generated from many different information system components. The list of audited events is the set of events for which audits are to be generated. These events are typically a subset of all events for which the information system is capable of generating audit records.

AU-13 MONITORING FOR INFORMATION DISCLOSURE

PCF Compliance

This requirement is an organizational responsibility and out of scope for the PCF platform. In addition, this requirement is categorized as P0, and so not required for [FISMA](#) Moderate.

Control Description


The organization monitors [Assignment: organization-defined open source information and/or information sites] [Assignment: organization-defined frequency] for evidence of unauthorized disclosure of organizational information.

Supplemental Guidance

Open source information includes, for example, social networking sites.

AU-14 SESSION AUDIT

PCF Compliance

This requirement is an organizational responsibility and out of scope for the PCF platform. It should be noted that additional security agents can be added to the PCF platform VMs as BOSH Add-ons, if and as needed. In addition, this requirement is categorized as P0, and so not required for [FISMA](#)  Moderate.

Control Description

The information system provides the capability for authorized users to select a user session to capture/record or view/hear.

Supplemental Guidance

Session audits include, for example, monitoring keystrokes, tracking websites visited, and recording information and/or file transfers. Session auditing activities are developed, integrated, and used in consultation with legal counsel in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, or standards.

AU-15 ALTERNATE AUDIT CAPABILITY

PCF Compliance

This requirement is an organizational responsibility and out of scope for the PCF platform. In addition, this requirement is categorized as P0, and so not required for [FISMA](#) Moderate.

Control Description

The organization provides an alternate audit capability in the event of a failure in primary audit capability that provides [Assignment: organization-defined alternate audit functionality].

Supplemental Guidance

Since an alternate audit capability may be a short-term protection employed until the failure in the primary auditing capability is corrected, organizations may determine that the alternate audit capability need only provide a subset of the primary audit functionality that is impacted by the failure.

AU-16 CROSS-ORGANIZATIONAL AUDITING

PCF Compliance

This requirement is an organizational responsibility and out of scope for the PCF platform. In addition, this requirement is categorized as P0, and so not required for [FISMA](#) Moderate.

Control Description

The organization employs [Assignment: organization-defined methods] for coordinating [Assignment: organization-defined audit information] among external organizations when audit information is transmitted across organizational boundaries.

Supplemental Guidance

When organizations use information systems and/or services of external organizations, the auditing capability necessitates a coordinated approach across organizations. For example, maintaining the identity of individuals that requested particular services across organizational boundaries may often be very difficult, and doing so may prove to have significant performance ramifications. Therefore, it is often the case that cross-organizational auditing (e.g., the type of auditing capability provided by service-oriented architectures) simply captures the identity of individuals issuing requests at the initial information system, and subsequent systems record that the requests emanated from authorized individuals.

AT - Awareness and Training Control Family

Number	Control	Pivotal Application Service (PAS) Compliance
AT-1	SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES	Inherited and Compliant
AT-2	SECURITY AWARENESS TRAINING	Deployer Responsibility
AT-3	ROLE-BASED SECURITY TRAINING	Deployer Responsibility
AT-4	SECURITY TRAINING RECORDS	Deployer Responsibility

AT-1 SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES

PCF Compliance

All xx-1 requirements are the responsibility of the deployer. The PCF product feature set is sufficient to satisfy the technical requirements implied in AT-1. Pivotal may be able to provide guidance to customers who are creating or updating documentation, but this documentation is unique to the deployer's mission and business goals.

Control Description

The organization:

- a. 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
- b. Reviews and updates the current:
 1. Security awareness and training policy [Assignment: organization-defined frequency]; and
 2. Security awareness and training procedures [Assignment: organization-defined frequency].

Supplemental Guidance

This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AT family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

AT-2 SECURITY AWARENESS TRAINING

PCF Compliance

Compliance with this requirement is the responsibility of the PCF deployer.

Control Description

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

- a. As part of initial training for new users;
- b. When required by information system changes; and
- c. [Assignment: organization-defined frequency] thereafter.

Supplemental Guidance

Organizations determine the appropriate content of security awareness training and security awareness techniques based on the specific organizational requirements and the information systems to which personnel have authorized access. The content includes a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents. The content also addresses awareness of the need for operations security. Security awareness techniques can include, for example, displaying posters, offering supplies inscribed with security reminders, generating email advisories/notices from senior organizational officials, displaying logon screen messages, and conducting information security awareness events.

AT-3 ROLE-BASED SECURITY TRAINING

PCF Compliance

Compliance with this requirement is the responsibility of the PCF deployer.

Control Description

The organization provides role-based security training to personnel with assigned security roles and responsibilities:

- a. Before authorizing access to the information system or performing assigned duties;
- b. When required by information system changes; and
- c. [Assignment: organization-defined frequency] thereafter.

Supplemental Guidance

Organizations determine the appropriate content of security training based on the assigned roles and responsibilities of individuals and the specific security requirements of organizations and the information systems to which personnel have authorized access. In addition, organizations provide enterprise architects, information system developers, software developers, acquisition/procurement officials, information system managers, system/network administrators, personnel conducting configuration management and auditing activities, personnel performing independent verification and validation activities, security control assessors, and other personnel having access to system-level software, adequate security-related technical training specifically tailored for their assigned duties. Comprehensive role-based training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical safeguards and countermeasures. Such training can include for example, policies, procedures, tools, and artifacts for the organizational security roles defined. Organizations also provide the training necessary for individuals to carry out their responsibilities related to operations and supply chain security within the context of organizational information security programs. Role-based security training also applies to contractors providing services to federal agencies.

AT-4 SECURITY TRAINING RECORDS

PCF Compliance

Compliance with this requirement is the responsibility of the PCF deployer.

Control Description

The organization:

- a. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and
- b. Retains individual training records for [Assignment: organization-defined time period].

Supplemental Guidance

Documentation for specialized training may be maintained by individual supervisors at the option of the organization.

CM - Configuration Management Control Family

Number	Control	Pivotal Application Service (PAS) Compliance
CM-1	CONFIGURATION MANAGEMENT POLICY AND PROCEDURES	Inherited and Compliant
CM-2	BASELINE CONFIGURATION	Inherited and Compliant
CM-3	CONFIGURATION CHANGE CONTROL	Inherited
CM-4	SECURITY IMPACT ANALYSIS	Inherited
CM-5	ACCESS RESTRICTIONS FOR CHANGE	Inherited
CM-6	CONFIGURATION SETTINGS	Inherited and Compliant
CM-7	LEAST FUNCTIONALITY	Inherited and Compliant
CM-8	INFORMATION SYSTEM COMPONENT INVENTORY	Inherited and Compliant
CM-9	CONFIGURATION MANAGEMENT PLAN	Inherited
CM-10	SOFTWARE USAGE RESTRICTIONS	Inherited
CM-11	USER-INSTALLED SOFTWARE	Inherited

CM-1 CONFIGURATION MANAGEMENT POLICY AND PROCEDURES

PCF Compliance

All xx-1 requirements are the responsibility of the deployer. The PCF product feature set is sufficient to satisfy the technical requirements implied in CM-1. Pivotal may be able to provide guidance to customers who are creating or updating documentation, but this documentation is unique to the deployer's mission and/or business goals.

Control Description

The organization:

- a. 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
- b. Reviews and updates the current:
 1. Configuration management policy [Assignment: organization-defined frequency]; and
 2. Configuration management procedures [Assignment: organization-defined frequency].

Supplemental Guidance

This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the CM family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

CM-2 BASELINE CONFIGURATION

PCF Compliance

All implied requirements are satisfied through a combination of PCF product features, and a deployer-provided version control system. Configuration management of the PCF deployment is provided through BOSH and Ops Manager. An operator may obtain a complete description of the PCF foundation by downloading a copy of the deployment manifests from the BOSH Director. It is a deployer responsibility maintain the associated configuration management policy and procedures documentation. Selection and use of a suitable version control system such as Git to maintain version control of deployment artifacts is a deployer responsibility.

Control Description

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

Supplemental Guidance

This control establishes baseline configurations for information systems and system components including communications and connectivity-related aspects of systems. Baseline configurations are documented, formally reviewed and agreed-upon sets of specifications for information systems or configuration items within those systems. Baseline configurations serve as a basis for future builds, releases, and/or changes to information systems. Baseline configurations include information about information system components (e.g., standard software packages installed on workstations, notebook computers, servers, network components, or mobile devices; current version numbers and patch information on operating systems and applications; and configuration settings/parameters), network topology, and the logical placement of those components within the system architecture. Maintaining baseline configurations requires creating new baselines as organizational information systems change over time. Baseline configurations of information systems reflect the current enterprise architecture.

CM-3 CONFIGURATION CHANGE CONTROL

PCF Compliance

Policies and procedures governing change control practices within the organization are the responsibility of the deployer. Changes made to a PCF deployment using BOSH or Ops Manager will be reflected in the deployment manifest, the BOSH director database, and the BOSH eventlog. The BOSH event log may be forwarded to an enterprise log management system. BOSH deployment manifests may be maintained in a version control system. An operator may also perform a manual comparison across different deployment manifest versions.

Control Description

The organization:

- a. Determines the types of changes to the information system that are configuration-controlled;
- b. Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses;
- c. Documents configuration change decisions associated with the information system;
- d. Implements approved configuration-controlled changes to the information system;
- e. Retains records of configuration-controlled changes to the information system for [Assignment: organization-defined time period];
- f. Audits and reviews activities associated with configuration-controlled changes to the information system; and
- g. Coordinates and provides oversight for configuration change control activities through [Assignment: organization-defined configuration change control element (e.g., committee, board)] that convenes [Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined configuration change conditions]].

Supplemental Guidance

Configuration change controls for organizational information systems involve the systematic proposal, justification, implementation, testing, review, and disposition of changes to the systems, including system upgrades and modifications. Configuration change control includes changes to baseline configurations for components and configuration items of information systems, changes to configuration settings for information technology products (e.g., operating systems, applications, firewalls, routers, and mobile devices), unscheduled/unauthorized changes, and changes to remediate vulnerabilities. Typical processes for managing configuration changes to information systems include, for example, Configuration Control Boards that approve proposed changes to systems. For new development information systems or systems undergoing major upgrades, organizations consider including representatives from development organizations on the Configuration Control Boards. Auditing of changes includes activities before and after changes are made to organizational information systems and the auditing activities required to implement such changes.

CM-4 SECURITY IMPACT ANALYSIS

PCF Compliance

Impact analysis to determine potential security implications of system changes are the responsibility of the deployer. The operational consistency provided by PCF helps to reduce the impact analysis of any planned changes. The use of PCF as a hosting environment enables organizations to achieve consistency in application deployment processes, reducing the need for extensive, application-specific impact analysis prior to application changes or upgrades. Changes to the PCF foundation itself are performed by an operator using BOSH or Ops Manager, and these actions can be performed while applications remain available. Changes to application configuration are not expected to have any impact on the security posture of the PCF platform infrastructure. The application isolation guarantees provided by the PCF platform help to reduce the impact of any planned application changes, and reduce the scope of any required impact analysis.

Control Description

The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.

Supplemental Guidance

Organizational personnel with information security responsibilities (e.g., Information System Administrators, Information System Security Officers, Information System Security Managers, and Information System Security Engineers) conduct security impact analyses. Individuals conducting security impact analyses possess the necessary skills/technical expertise to analyze the changes to information systems and the associated security ramifications. Security impact analysis may include, for example, reviewing security plans to understand security control requirements and reviewing system design documentation to understand control implementation and how specific changes might affect the controls. Security impact analyses may also include assessments of risk to better understand the impact of the changes and to determine if additional security controls are required. Security impact analyses are scaled in accordance with the security categories of the information systems.

CM-5 ACCESS RESTRICTIONS FOR CHANGE

PCF Compliance

Physical access restrictions are the responsibility of the deployer. PCF provides logical access controls for operators using BOSH and Ops Manager performing change management functions on the platform.

For example, authentication to BOSH and Ops Manager may be controlled using integration of UAA and the existing enterprise- or agency-deployed Identity Management system. BOSH and Ops Manager must be deployed on a restricted management subnet, and access controlled through a bastion host (Jumpbox) as described in the reference architecture. As of PCF v2.1, Ops Manager users with Full View and Restricted View permissions can be logged in simultaneously. Prior to this release, only one user at a time could view Ops Manager. For security purposes, operators with write access still cannot be logged into Ops Manager simultaneously. Additional procedural controls to ensure only one Ops Manager user with write access at any one time is a deployer responsibility.

Logical access controls to protect change management of deployed applications are provided by the RBAC capabilities of the Cloud Controller. Refer to the associated documentation pages for more information about Cloud Controller RBAC.

Control Description

The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.

Supplemental Guidance

Any changes to the hardware, software, and/or firmware components of information systems can potentially have significant effects on the overall security of the systems. Therefore, organizations permit only qualified and authorized individuals to access information systems for purposes of initiating changes, including upgrades and modifications. Organizations maintain records of access to ensure that configuration change control is implemented and to support after-the-fact actions should organizations discover any unauthorized changes. Access restrictions for change also include software libraries. Access restrictions include, for example, physical and logical access controls (see AC-3 and PE-3), workflow automation, media libraries, abstract layers (e.g., changes implemented into third-party interfaces rather than directly into information systems), and change windows (e.g., changes occur only during specified times, making unauthorized changes easy to discover).

CM-6 CONFIGURATION SETTINGS

PCF Compliance

The technical configuration settings for a PCF deployment are managed by BOSH and Ops Manager. An operator may choose to place BOSH manifests under external version control. Similarly for applications that are deployed on the PCF platform. Application artifacts may be placed under version control as needed. Any required procedural controls that protect access to the versioned manifest artifacts are a deployer responsibility. All implied requirements are satisfied.

Details

deployer responsibility

Control Description

The organization:

- a. Establishes and documents configuration settings for information technology products employed within the information system using [Assignment: organization-defined security configuration checklists] that reflect the most restrictive mode consistent with operational requirements;
- b. Implements the configuration settings;
- c. 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
- d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

Supplemental Guidance

Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the information system that affect the security posture and/or functionality of the system. Information technology products for which security-related configuration settings can be defined include, for example, mainframe computers, servers (e.g., database, electronic mail, authentication, web, proxy, file, domain name), workstations, input/output devices (e.g., scanners, copiers, and printers), network components (e.g., firewalls, routers, gateways, voice and data switches, wireless access points, network appliances, sensors), operating systems, middleware, and applications. Security-related parameters are those parameters impacting the security state of information systems including the parameters required to satisfy other security control requirements. Security-related parameters include, for example: (i) registry settings; (ii) account, file, directory permission settings; and (iii) settings for functions, ports, protocols, services, and remote connections. Organizations establish organization-wide configuration settings and subsequently derive specific settings for information systems. The established settings become part of the systems configuration baseline. Common secure configurations (also referred to as security configuration checklists, lockdown and hardening guides, security reference guides, security technical implementation guides) provide recognized, standardized, and established benchmarks that stipulate secure configuration settings for specific information technology platforms/products and instructions for configuring those information system components to meet operational requirements. Common secure configurations can be developed by a variety of organizations including, for example, information technology product developers, manufacturers, vendors, consortia, academia, industry, federal agencies, and other organizations in the public and private sectors. Common secure configurations include the United States Government Configuration Baseline (USGCB) which affects the implementation of CM-6 and other controls such as AC-19 and CM-7. The Security Content Automation Protocol (SCAP) and the defined standards within the protocol (e.g., Common Configuration Enumeration) provide an effective method to uniquely identify, track, and control configuration settings. OMB establishes federal policy on configuration requirements for federal information systems.

CM-7 LEAST FUNCTIONALITY

PCF Compliance

When the PCF platform is deployed in accordance with the reference architecture guidance the platform is compliant. System functions, ports, protocols, and services are exposed only as needed and appropriate for the platform operation. In particular, the reference architecture requires that the CF Router provide the entry point to the deployment for users and operators. The other VMs that make up the PAS runtime environment are not routable from the enterprise network. There are no unnecessary functions, ports, protocols, or services exposed that are not strictly required. Deployers have the option of turning off access through SSH. Deployers have the option of requiring TLS for access to public endpoints. The BOSH stemcell is hardened to remove unneeded functions, ports, protocols and services. The PCF configuration options include a number of feature flags that may be enabled at the deployer's discretion. It is a deployer responsibility to configure these options if and as needed.

Control Description

The organization:

- a. Configures the information system to provide only essential capabilities; and
- b. Prohibits or restricts the use of the following functions, ports, protocols, and/or services: [Assignment: organization-defined prohibited or restricted functions, ports, protocols, and/or services].

Supplemental Guidance

Information systems can provide a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions). Additionally, it is sometimes convenient to provide multiple services from single information system components, but doing so increases risk over limiting the services provided by any one component. Where feasible, organizations limit component functionality to a single function per device (e.g., email servers or web servers, but not both). Organizations review functions and services provided by information systems or individual components of information systems, to determine which functions and services are candidates for elimination (e.g., Voice Over Internet Protocol, Instant Messaging, auto-execute, and file sharing). Organizations consider disabling unused or unnecessary physical and logical ports/protocols (e.g., Universal Serial Bus, File Transfer Protocol, and Hyper Text Transfer Protocol) on information systems to prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling. Organizations can utilize network scanning tools, intrusion detection and prevention systems, and end-point protections such as firewalls and host-based intrusion detection systems to identify and prevent the use of prohibited functions, ports, protocols, and services.

CM-8 INFORMATION SYSTEM COMPONENT INVENTORY

PCF Compliance

This requirement is satisfied by BOSH and Ops Manager, along with the underlying IaaS console, which enable the deployer to generate a full component inventory for all assets in the deployment if and as needed. The associated policies and procedures are a deployer responsibility. All implied requirements are satisfied.

Control Description

The organization:

- a. 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
- b. Reviews and updates the information system component inventory [Assignment: organization-defined frequency].

Supplemental Guidance

Organizations may choose to implement centralized information system component inventories that include components from all organizational information systems. In such situations, organizations ensure that the resulting inventories include system-specific information required for proper component accountability (e.g., information system association, information system owner). Information deemed necessary for effective accountability of information system components includes, for example, hardware inventory specifications, software license information, software version numbers, component owners, and for networked components or devices, machine names and network addresses. Inventory specifications include, for example, manufacturer, device type, model, serial number, and physical location.

CM-9 CONFIGURATION MANAGEMENT PLAN

PCF Compliance

This requirement is a deployer responsibility. All implied requirements are satisfied.

Control Description

- a. Addresses roles, responsibilities, and configuration management processes and procedures;
- b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;
- c. Defines the configuration items for the information system and places the configuration items under configuration management; and
- d. Protects the configuration management plan from unauthorized disclosure and modification.

Supplemental Guidance

Configuration management plans satisfy the requirements in configuration management policies while being tailored to individual information systems. Such plans define detailed processes and procedures for how configuration management is used to support system development life cycle activities at the information system level. Configuration management plans are typically developed during the development/acquisition phase of the system development life cycle. The plans describe how to move changes through change management processes, how to update configuration settings and baselines, how to maintain information system component inventories, how to control development, test, and operational environments, and how to develop, release, and update key documents. Organizations can employ templates to help ensure consistent and timely development and implementation of configuration management plans. Such templates can represent a master configuration management plan for the organization at large with subsets of the plan implemented on a system by system basis. Configuration management approval processes include designation of key management stakeholders responsible for reviewing and approving proposed changes to information systems, and personnel that conduct security impact analyses prior to the implementation of changes to the systems. Configuration items are the information system items (hardware, software, firmware, and documentation) to be configuration-managed. As information systems continue through the system development life cycle, new configuration items may be identified and some existing configuration items may no longer need to be under configuration control.

CM-10 SOFTWARE USAGE RESTRICTIONS

PCF Compliance

This requirement is a deployer responsibility. All implied requirements are satisfied.

Control Description

The organization:

- a. Uses software and associated documentation in accordance with contract agreements and copyright laws;
- b. Tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution; and
- c. 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.

Supplemental Guidance

Software license tracking can be accomplished by manual methods (e.g., simple spreadsheets) or automated methods (e.g., specialized tracking applications) depending on organizational needs.

CM-11 USER-INSTALLED SOFTWARE

PCF Compliance

This requirement is a deployer responsibility. All implied requirements are satisfied. Developers with appropriate RBAC Cloud Controller roles assigned to their account may perform a `cf push` operation to run application code on the foundation. However, all application code is executed within a container environment and is not permitted access to the host VMs.

Control Description

- a. Establishes [Assignment: organization-defined policies] governing the installation of software by users;
- b. Enforces software installation policies through [Assignment: organization-defined methods]; and
- c. Monitors policy compliance at [Assignment: organization-defined frequency].

Supplemental Guidance

If provided the necessary privileges, users have the ability to install software in organizational information systems. To maintain control over the types of software installed, organizations identify permitted and prohibited actions regarding software installation. Permitted software installations may include, for example, updates and security patches to existing software and downloading applications from organization-approved “app stores.” Prohibited software installations may include, for example, software with unknown or suspect pedigrees or software that organizations consider potentially malicious. The policies organizations select governing user-installed software may be organization-developed or provided by some external entity. Policy enforcement methods include procedural methods (e.g., periodic examination of user accounts), automated methods (e.g., configuration settings implemented on organizational information systems), or both.

CP - Contingency Planning Control Family

Number	Control	Pivotal Application Service (PAS) Compliance
CP-1	CONTINGENCY PLANNING POLICY AND PROCEDURES	Inherited and Compliant
CP-2	CONTINGENCY PLAN	Inherited
CP-3	CONTINGENCY TRAINING	Inherited
CP-4	CONTINGENCY PLAN TESTING	Inherited
CP-5	CONTINGENCY PLAN UPDATE	[Withdrawn: Incorporated into CP-2]
CP-6	ALTERNATE STORAGE SITE	Inherited and Compliant
CP-7	ALTERNATE PROCESSING SITE	Inherited and Compliant
CP-8	TELECOMMUNICATIONS SERVICES	Inherited
CP-9	INFORMATION SYSTEM BACKUP	Inherited and Compliant
CP-10	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION	Inherited
CP-11	ALTERNATE COMMUNICATIONS PROTOCOLS	P0, so not required for FISMA Moderate
CP-12	SAFE MODE	P0, so not required for FISMA Moderate
CP-13	ALTERNATIVE SECURITY MECHANISMS	P0, so not required for FISMA Moderate

CP-1 CONTINGENCY PLANNING POLICY AND PROCEDURES

PCF Compliance

All dash-1 requirements are the responsibility of the deployer. Pivotal may be able to provide guidance to customers who are creating or updating documentation, but this documentation is unique to the deployer's mission and business goals. All implied requirements are satisfied. PCF features are sufficient to satisfy CP-1.

Control Description

The organization:

- a. 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
- b. Reviews and updates the current:
 1. Contingency planning policy [Assignment: organization-defined frequency]; and
 2. Contingency planning procedures [Assignment: organization-defined frequency].

Supplemental Guidance

This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the CP family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

CP-2 CONTINGENCY PLAN

PCF Compliance

Compliance with this requirement is the responsibility of the PCF deployer.

Contingency plans can incorporate:

- The [BOSH Backup and Restore](#) tool to recover PCF deployments.
- The [Concourse](#) continuous integration and continuous delivery (CI/CD) tool to automatically rebuild and run tests on PCF deployments.

Control Description

The organization:

- a. 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];
- b. Distributes copies of the contingency plan to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements];
- c. Coordinates contingency planning activities with incident handling activities;
- d. Reviews the contingency plan for the information system [Assignment: organization-defined frequency];
- e. 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;
- f. Communicates contingency plan changes to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]; and
- g. Protects the contingency plan from unauthorized disclosure and modification.

Supplemental Guidance

Contingency planning for information systems is part of an overall organizational program for achieving continuity of operations for mission/business functions. Contingency planning addresses both information system restoration and implementation of alternative mission/business processes when systems are compromised. The effectiveness of contingency planning is maximized by considering such planning throughout the phases of the system development life cycle. Performing contingency planning on hardware, software, and firmware development can be an effective means of achieving information system resiliency. Contingency plans reflect the degree of restoration required for organizational information systems since not all systems may need to fully recover to achieve the level of continuity of operations desired. Information system recovery objectives reflect applicable laws, Executive Orders, directives, policies, standards, regulations, and guidelines. In addition to information system availability, contingency plans also address other security-related events resulting in a reduction in mission and/or business effectiveness, such as malicious attacks compromising the confidentiality or integrity of information systems. Actions addressed in contingency plans include, for example, orderly/graceful degradation, information system shutdown, fallback to a manual mode, alternate information flows, and operating in modes reserved for when systems are under attack. By closely coordinating contingency planning with incident handling activities, organizations can ensure that the necessary contingency planning activities are in place and activated in the event of a security incident.

CP-3 CONTINGENCY TRAINING

PCF Compliance

Compliance with this requirement is the responsibility of the PCF deployer.

Control Description

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

- a. Within [Assignment: organization-defined time period] of assuming a contingency role or responsibility;
- b. When required by information system changes; and
- c. [Assignment: organization-defined frequency] thereafter.

Supplemental Guidance

Contingency training provided by organizations is linked to the assigned roles and responsibilities of organizational personnel to ensure that the appropriate content and level of detail is included in such training. For example, regular users may only need to know when and where to report for duty during contingency operations and if normal duties are affected; system administrators may require additional training on how to set up information systems at alternate processing and storage sites; and managers/senior leaders may receive more specific training on how to conduct mission-essential functions in designated off-site locations and how to establish communications with other governmental entities for purposes of coordination on contingency-related activities. Training for contingency roles/responsibilities reflects the specific continuity requirements in the contingency plan.

CP-4 CONTINGENCY PLAN TESTING

PCF Compliance

Compliance with this requirement is the responsibility of the PCF deployer.

Control Description

The organization:

- a. Tests the contingency plan for the information system [Assignment: organization-defined frequency] using [Assignment: organization-defined tests] to determine the effectiveness of the plan and the organizational readiness to execute the plan;
- b. Reviews the contingency plan test results; and
- c. Initiates corrective actions, if needed.

Supplemental Guidance

Methods for testing contingency plans to determine the effectiveness of the plans and to identify potential weaknesses in the plans include, for example, walk-through and tabletop exercises, checklists, simulations (parallel, full interrupt), and comprehensive exercises. Organizations conduct testing based on the continuity requirements in contingency plans and include a determination of the effects on organizational operations, assets, and individuals arising due to contingency operations. Organizations have flexibility and discretion in the breadth, depth, and timelines of corrective actions.

CP-5 CONTINGENCY PLAN UPDATE

Control Description

[Withdrawn: Incorporated into CP-2]

Supplemental Guidance

CP-6 ALTERNATE STORAGE SITE

PCF Compliance

When deployed in accordance with the reference architecture, PCF is compliant with this requirement. If the infrastructure supports it, PAS can operate across multiple availability zones (AZs). Applications deployed to the platform inherit this redundancy across availability zones.

PCF applications store their data by binding to data services, and whether these data are stored in multiple sites depends on how these services are configured.

A contingency plan can support an alternate storage site for PCF using the [BOSH Backup and Restore](#) tool to recover PCF deployments.

Control Description

The organization:

- a. Establishes an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information;
and
- b. Ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site.

Supplemental Guidance

Alternate storage sites are sites that are geographically distinct from primary storage sites. An alternate storage site maintains duplicate copies of information and data in the event that the primary storage site is not available. Items covered by alternate storage site agreements include, for example, environmental conditions at alternate sites, access rules, physical and environmental protection requirements, and coordination of delivery/retrieval of backup media. Alternate storage sites reflect the requirements in contingency plans so that organizations can maintain essential missions/business functions despite disruption, compromise, or failure in organizational information systems.

CP-7 ALTERNATE PROCESSING SITE

PCF Compliance

When deployed in accordance with the reference architecture, PCF is compliant with this requirement. If the infrastructure supports it, PAS can operate across multiple availability zones (AZs). Applications deployed to the platform inherit this redundancy across availability zones.

Note that BOSH and Ops Manager are deployed to a single AZ, but any unplanned downtime of these management plane components does not impact application availability.

Control Description

The organization:

- a. 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 [Assignment: organization-defined time period consistent with recovery time and recovery point objectives] when the primary processing capabilities are unavailable;
- b. 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
- c. Ensures that the alternate processing site provides information security safeguards equivalent to those of the primary site.

Supplemental Guidance

Alternate processing sites are sites that are geographically distinct from primary processing sites. An alternate processing site provides processing capability in the event that the primary processing site is not available. Items covered by alternate processing site agreements include, for example, environmental conditions at alternate sites, access rules, physical and environmental protection requirements, and coordination for the transfer/assignment of personnel. Requirements are specifically allocated to alternate processing sites that reflect the requirements in contingency plans to maintain essential missions/business functions despite disruption, compromise, or failure in organizational information systems.

CP-8 TELECOMMUNICATIONS SERVICES

PCF Compliance

Compliance with this requirement is the responsibility of the PCF deployer.

Control Description

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 [Assignment: organization-defined time period] when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

Supplemental Guidance

This control applies to telecommunications services (data and voice) for primary and alternate processing and storage sites. Alternate telecommunications services reflect the continuity requirements in contingency plans to maintain essential missions/business functions despite the loss of primary telecommunications services. Organizations may specify different time periods for primary/alternate sites. Alternate telecommunications services include, for example, additional organizational or commercial ground-based circuits/lines or satellites in lieu of ground-based communications. Organizations consider factors such as availability, quality of service, and access when entering into alternate telecommunications agreements.

CP-9 INFORMATION SYSTEM BACKUP

PCF Compliance

Compliance with this requirement is the responsibility of the PCF deployer.

PCF provides system backup support through [BOSH Backup and Restore](#).

Control Description

The organization:

- a. Conducts backups of user-level information contained in the information system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives];
- b. Conducts backups of system-level information contained in the information system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives];
- c. Conducts backups of information system documentation including security-related documentation [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; and
- d. Protects the confidentiality, integrity, and availability of backup information at storage locations.

Supplemental Guidance

System-level information includes, for example, system-state information, operating system and application software, and licenses. User-level information includes any information other than system-level information. Mechanisms employed by organizations to protect the integrity of information system backups include, for example, digital signatures and cryptographic hashes. Protection of system backup information while in transit is beyond the scope of this control. Information system backups reflect the requirements in contingency plans as well as other organizational requirements for backing up information.

CP-10 INFORMATION SYSTEM RECOVERY AND RECONSTITUTION

PCF Compliance

Compliance with this requirement is the responsibility of the PCF deployer.

PCF supports system recovery and reconstitution through the [BOSH Backup and Restore](#) tool.

Control Description

The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.

Supplemental Guidance

Recovery is executing information system contingency plan activities to restore organizational missions/business functions. Reconstitution takes place following recovery and includes activities for returning organizational information systems to fully operational states. Recovery and reconstitution operations reflect mission and business priorities, recovery point/time and reconstitution objectives, and established organizational metrics consistent with contingency plan requirements. Reconstitution includes the deactivation of any interim information system capabilities that may have been needed during recovery operations. Reconstitution also includes assessments of fully restored information system capabilities, reestablishment of continuous monitoring activities, potential information system reauthorizations, and activities to prepare the systems against future disruptions, compromises, or failures. Recovery/reconstitution capabilities employed by organizations can include both automated mechanisms and manual procedures.

CP-11 ALTERNATE COMMUNICATIONS PROTOCOLS

PCF Compliance

P0, so not required.

Control Description

The information system provides the capability to employ [Assignment: organization-defined alternative communications protocols] in support of maintaining continuity of operations.

Supplemental Guidance

Contingency plans and the associated training and testing for those plans, incorporate an alternate communications protocol capability as part of increasing the resilience of organizational information systems. Alternate communications protocols include, for example, switching from Transmission Control Protocol/Internet Protocol (TCP/IP) Version 4 to TCP/IP Version 6. Switching communications protocols may affect software applications and therefore, the potential side effects of introducing alternate communications protocols are analyzed prior to implementation.

CP-12 SAFE MODE

PCF Compliance

PO, so not required.

Control Description

The information system, when [Assignment: organization-defined conditions] are detected, enters a safe mode of operation with [Assignment: organization-defined restrictions of safe mode of operation].

Supplemental Guidance

For information systems supporting critical missions/business functions including, for example, military operations and weapons systems, civilian space operations, nuclear power plant operations, and air traffic control operations (especially real-time operational environments), organizations may choose to identify certain conditions under which those systems revert to a predefined safe mode of operation. The safe mode of operation, which can be activated automatically or manually, restricts the types of activities or operations information systems could execute when those conditions are encountered. Restriction includes, for example, allowing only certain functions that could be carried out under limited power or with reduced communications bandwidth.

CP-13 ALTERNATIVE SECURITY MECHANISMS

PCF Compliance

PO, so not required.

Control Description

The organization employs [Assignment: organization-defined alternative or supplemental security mechanisms] for satisfying [Assignment: organization-defined security functions] when the primary means of implementing the security function is unavailable or compromised.

Supplemental Guidance

This control supports information system resiliency and contingency planning/continuity of operations. To ensure mission/business continuity, organizations can implement alternative or supplemental security mechanisms. These mechanisms may be less effective than the primary mechanisms (e.g., not as easy to use, not as scalable, or not as secure). However, having the capability to readily employ these alternative/supplemental mechanisms enhances overall mission/business continuity that might otherwise be adversely impacted if organizational operations had to be curtailed until the primary means of implementing the functions was restored. Given the cost and level of effort required to provide such alternative capabilities, this control would typically be applied only to critical security capabilities provided by information systems, system components, or information system services. For example, an organization may issue to senior executives and system administrators one-time pads in case multifactor tokens, the organization's standard means for secure remote authentication, is compromised.

IA - Identification and Authentication Control Family

Number	Control	Pivotal Application Service (PAS) Compliance
IA-1	IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES	Deployer responsibility
IA-2	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)	compliant and inherited
IA-3	DEVICE IDENTIFICATION AND AUTHENTICATION	compliant and inherited
IA-4	IDENTIFIER MANAGEMENT	compliant
IA-5	AUTHENTICATOR MANAGEMENT	Deployer responsibility
IA-6	AUTHENTICATOR FEEDBACK	compliant
IA-7	CRYPTOGRAPHIC MODULE AUTHENTICATION	partially compliant
IA-8	IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)	compliant
IA-9	SERVICE IDENTIFICATION AND AUTHENTICATION	P0, so not required for FISMA moderate
IA-10	ADAPTIVE IDENTIFICATION AND AUTHENTICATION	P0, so not required for FISMA moderate
IA-11	RE-AUTHENTICATION	P0, so not required for FISMA moderate

IA-1 IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES

PCF Compliance

All xx-1 requirements are the responsibility of the deployer. The PCF product feature set is sufficient to satisfy the technical requirements implied in IA-1. Pivotal may be able to provide guidance to customers who are creating or updating documentation, but this documentation is unique to the deployer's mission and/or business goals.

Control Description

The organization:

- a. 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
- b. Reviews and updates the current:
 1. Identification and authentication policy [Assignment: organization-defined frequency]; and
 2. Identification and authentication procedures [Assignment: organization-defined frequency].

Supplemental Guidance

This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the IA family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

IA-2 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)

PCF Compliance

When deployed in accordance with the recommended reference architecture the PCF platform is compliant with this requirement. The entry point to access any services in the PCF platform are the Cloud Controller (for developers) and the BOSH director and/or Ops Manager (for operators).

Both of these end points require authentication at UAA before any further action may be taken. The UAA may be configured to delegate the initial user authentication requirement to an enterprise IdM, including LDAP and/or SAML authentication.

When multi-factor authentication is required, a deployer may configure the IdM system to require multifactor authentication prior to the issuance of a SAML assertion, which would then be presented at the UAA. Support for PIV or CAC authentication is delegated to the enterprise IdM.

Developers and operators are only required to authenticate once to access their respective service end points. Note, however, that any single individual that needs to perform both developer and operator functions would be required to establish a new session for each of these distinct roles. This behavior enables appropriate Separation of Duties for deployments that require this.

Support for Single Sign-On functionality across multiple deployed applications is available as a service for any applications that chose to use it.

Control Description

The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

Supplemental Guidance

Organizational users include employees or individuals that organizations deem to have equivalent status of employees (e.g., contractors, guest researchers). This control applies to all accesses other than: (i) accesses that are explicitly identified and documented in AC-14; and (ii) accesses that occur through authorized use of group authenticators without individual authentication. Organizations may require unique identification of individuals in group accounts (e.g., shared privilege accounts) or for detailed accountability of individual activity. Organizations employ passwords, tokens, or biometrics to authenticate user identities, or in the case multifactor authentication, or some combination thereof. Access to organizational information systems is defined as either local access or network access. Local access is any access to organizational information systems by users (or processes acting on behalf of users) where such access is obtained by direct connections without the use of networks. Network access is access to organizational information systems by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks (e.g., the Internet). Internal networks include local area networks and wide area networks. In addition, the use of encrypted virtual private networks (VPNs) for network connections between organization-controlled endpoints and non-organization controlled endpoints may be treated as internal networks from the perspective of protecting the confidentiality and integrity of information traversing the network. Organizations can satisfy the identification and authentication requirements in this control by complying with the requirements in Homeland Security Presidential Directive 12 consistent with the specific organizational implementation plans. Multifactor authentication requires the use of two or more different factors to achieve authentication. The factors are defined as: (i) something you know (e.g., password, personal identification number [PIN]); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card and the DoD common access card. In addition to identifying and authenticating users at the information system level (i.e., at logon), organizations also employ identification and authentication mechanisms at the application level, when necessary, to provide increased information security. Identification and authentication requirements for other than organizational users are described in IA-8.

IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION

PCF Compliance

The VMs that are created in a PCF deployment are created by BOSH on existing IAAS infrastructure, on a designated private subnet.

All devices “admitted” to this subnet are determined by the authorized BOSH operator. e.g. there is no provision for an externally managed device to obtain an address on the private subnet via, e.g. DHCP and EAP. In addition, the controlled distribution of IPsec credentials prevents any externally managed VMs from communicating on the PAS private subnet.

Admittance of end user client devices to a network that is routable to PCF is the responsibility of the deployer.

Control Description

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.

Supplemental Guidance

Organizational devices requiring unique device-to-device identification and authentication may be defined by type, by device, or by a combination of type/device. Information systems typically use either shared known information (e.g., Media Access Control [MAC] or Transmission Control Protocol/Internet Protocol [TCP/IP] addresses) for device identification or organizational authentication solutions (e.g., IEEE 802.1x and Extensible Authentication Protocol [EAP], Radius server with EAP-Transport Layer Security [TLS] authentication, Kerberos) to identify/authenticate devices on local and/or wide area networks. Organizations determine the required strength of authentication mechanisms by the security categories of information systems. Because of the challenges of applying this control on large scale, organizations are encouraged to only apply the control to those limited number (and type) of devices that truly need to support this capability.

IA-4 IDENTIFIER MANAGEMENT

PCF Compliance

Identifiers for components within the PCF deployment are managed by BOSH, and the underlying Cloud Provider Interface (CPI). With High Probability, all identifiers are unique in a deployment, and not shared or reused. At the time of a new BOSH deployment, it is expected that, e.g. IP addresses in the CIDR range of the PAS private subnet may be reused. However, the BOSH director ensures that each IP address in the CIDE subnet will be uniquely assigned for a given deployment operation. Assignment of host identifiers is visible in audit logs of the BOSH director, PCF, and/or the CPI.

Identifiers used by external entities such as end users or end user devices are the responsibility of the deployer.

Control Description

The organization manages information system identifiers by:

- a. Receiving authorization from [Assignment: organization-defined personnel or roles] to assign an individual, group, role, or device identifier;
- b. Selecting an identifier that identifies an individual, group, role, or device;
- c. Assigning the identifier to the intended individual, group, role, or device;
- d. Preventing reuse of identifiers for [Assignment: organization-defined time period]; and
- e. Disabling the identifier after [Assignment: organization-defined time period of inactivity].

Supplemental Guidance

Common device identifiers include, for example, media access control (MAC), Internet protocol (IP) addresses, or device-unique token identifiers. Management of individual identifiers is not applicable to shared information system accounts (e.g., guest and anonymous accounts). Typically, individual identifiers are the user names of the information system accounts assigned to those individuals. In such instances, the account management activities of AC-2 use account names provided by IA-4. This control also addresses individual identifiers not necessarily associated with information system accounts (e.g., identifiers used in physical security control databases accessed by badge reader systems for access to information systems). Preventing reuse of identifiers implies preventing the assignment of previously used individual, group, role, or device identifiers to different individuals, groups, roles, or devices.

IA-5 AUTHENTICATOR MANAGEMENT

PCF Compliance

End User authenticator management is the responsibility of the deployer.

Intra-platform authenticator management is the responsibility of BOSH and Ops Man and CredHub. Rotating intra-system authenticators in PAS is a supported procedure.

It is not yet fully automated, but may be accomplished through manual intervention.

It is a deployer responsibility to align organizational policy and operational procedures to supplement native PCF capabilities if and as needed.

Validation of end user PKI credentials is delegated to the enterprise IdM.

Validation of intra-platform PKI credentials uses the deployer-configured CA trust chain. However, there is no OCSP or CRL checking for intra-platform PKI credentials.

The strategy for avoiding reliance on a compromised credential is based upon frequent rotation of short lived credentials.

Control Description

The organization manages information system authenticators by:

- a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;
- b. Establishing initial authenticator content for authenticators defined by the organization;
- c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;
- d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;
- e. Changing default content of authenticators prior to information system installation;
- f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;
- g. Changing/refreshing authenticators [Assignment: organization-defined time period by authenticator type];
- h. Protecting authenticator content from unauthorized disclosure and modification;
- i. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and
- j. Changing authenticators for group/role accounts when membership to those accounts changes.

Supplemental Guidance

Individual authenticators include, for example, passwords, tokens, biometrics, PKI certificates, and key cards. Initial authenticator content is the actual content (e.g., the initial password) as opposed to requirements about authenticator content (e.g., minimum password length). In many cases, developers ship information system components with factory default authentication credentials to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, and present a significant security risk. The requirement to protect individual authenticators may be implemented via control PL-4 or PS-6 for authenticators in the possession of individuals and by controls AC-3, AC-6, and SC-28 for authenticators stored within organizational information systems (e.g., passwords stored in hashed or encrypted formats, files containing encrypted or hashed passwords accessible with administrator privileges). Information systems support individual authenticator management by organization-defined settings and restrictions for various authenticator characteristics including, for example, minimum password length, password composition, validation time window for time synchronous one-time tokens, and number of allowed rejections during the verification stage of biometric authentication. Specific actions that can be taken to safeguard authenticators include, for example, maintaining possession of individual authenticators, not loaning or sharing individual authenticators with others, and reporting lost, stolen, or compromised authenticators immediately. Authenticator management includes issuing and revoking, when no longer needed, authenticators for temporary access such as that required for remote maintenance. Device authenticators include, for example, certificates and passwords.

IA-6 AUTHENTICATOR FEEDBACK

PCF Compliance

All PCF authentication functions support a compliant operational mode.

Graphical user interfaces, as well as CLI endpoints provide credential masking capabilities if and as needed. It is a deployer responsibility to leverage these features as appropriate.

Control Description

The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

Supplemental Guidance

The feedback from information systems does not provide information that would allow unauthorized individuals to compromise authentication mechanisms. For some types of information systems or system components, for example, desktops/notebooks with relatively large monitors, the threat (often referred to as shoulder surfing) may be significant. For other types of systems or components, for example, mobile devices with 2-4 inch screens, this threat may be less significant, and may need to be balanced against the increased likelihood of typographic input errors due to the small keyboards. Therefore, the means for obscuring the authenticator feedback is selected accordingly. Obscuring the feedback of authentication information includes, for example, displaying asterisks when users type passwords into input devices, or displaying feedback for a very limited time before fully obscuring it.

IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION

PCF Compliance

Not all cryptographic modules present in a PCF deployment are FIPS compliant.

The cryptographic modules deployed for IPsec communication (OpenSSL, C language) are built and deployed to operate in FIPS mode. However, the cryptographic modules used in UAA (Java), the CF router, and Diego (Golang), as well as the OpenSSL package used for host-based SSH (C language), are not currently FIPS compliant.

Control Description

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.

Supplemental Guidance

Authentication mechanisms may be required within a cryptographic module to authenticate an operator accessing the module and to verify that the operator is authorized to assume the requested role and perform services within that role.

IA-8 IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)

PCF Compliance

All functions and services within a PCF deployment require appropriate authentication via UAA. The UAA supports identify federation via the SAMLv2 standard. The UAA also supports the configuration of Identity Provider discovery. This means that users may authenticate via email addresses from different DNS domains. Users from the different domains will be redirected to their respective IDP, as appropriate.

Control Description

The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).

Supplemental Guidance

Non-organizational users include information system users other than organizational users explicitly covered by IA-2. These individuals are uniquely identified and authenticated for accesses other than those accesses explicitly identified and documented in AC-14. In accordance with the E-Authentication E-Government initiative, authentication of non-organizational users accessing federal information systems may be required to protect federal, proprietary, or privacy-related information (with exceptions noted for national security systems). Organizations use risk assessments to determine authentication needs and consider scalability, practicality, and security in balancing the need to ensure ease of use for access to federal information and information systems with the need to protect and adequately mitigate risk. IA-2 addresses identification and authentication requirements for access to information systems by organizational users.

IA-9 SERVICE IDENTIFICATION AND AUTHENTICATION

PCF Compliance

The PCF platform itself is compliant with this requirement. As a distributed-computing cloud-native platform, PCF implements appropriate identification and authentication capabilities for all communications that occur within the platform, between distributed platform jobs, such as Diego, Cloud Controller, UAA, and so on.

Compliance with this requirement for hosted applications and user-provided services is the responsibility of the deployer.

Control Description

The organization identifies and authenticates [Assignment: organization-defined information system services] using [Assignment: organization-defined security safeguards].

Supplemental Guidance

This control supports service-oriented architectures and other distributed architectural approaches requiring the identification and authentication of information system services. In such architectures, external services often appear dynamically. Therefore, information systems should be able to determine in a dynamic manner, if external providers and associated services are authentic. Safeguards implemented by organizational information systems to validate provider and service authenticity include, for example, information or code signing, provenance graphs, and/or electronic signatures indicating or including the sources of services.

IA-10 ADAPTIVE IDENTIFICATION AND AUTHENTICATION

PCF Compliance

This requirement is P0, and not required for FISMA moderate. Organizations that choose to adopt adaptive identification and authentication capabilities may do so via delegation of this requirement to their existing Identity Management infrastructure. For example, a deployer may choose to require adaptive authentication at the IDP prior to issuance of a SAML assertion. The user accessing PCF will be required to present a valid assertion, however the authentication mechanism required to obtain that assertion is considered out of scope from the perspective of the PCF platform as the relying party.

Control Description

The organization requires that individuals accessing the information system employ [Assignment: organization-defined supplemental authentication techniques or mechanisms] under specific [Assignment: organization-defined circumstances or situations].

Supplemental Guidance

Adversaries may compromise individual authentication mechanisms and subsequently attempt to impersonate legitimate users. This situation can potentially occur with any authentication mechanisms employed by organizations. To address this threat, organizations may employ specific techniques/mechanisms and establish protocols to assess suspicious behavior (e.g., individuals accessing information that they do not typically access as part of their normal duties, roles, or responsibilities, accessing greater quantities of information than the individuals would routinely access, or attempting to access information from suspicious network addresses). In these situations when certain preestablished conditions or triggers occur, organizations can require selected individuals to provide additional authentication information. Another potential use for adaptive identification and authentication is to increase the strength of mechanism based on the number and/or types of records being accessed.

IA-11 RE-AUTHENTICATION

PCF Compliance

This requirement is P0, and not required for FISMA moderate.

Access to all PCF platform functions is via tokens issued from UAA. Once issued, these tokens enable the user to establish a session at a specific PCF end point interface, such as a Web session with Apps Manager, or a CF CLI session from a command prompt. User session timeouts have default values, and these default values may be overridden by the deployer if and as needed. Upon session timeout, the user is required to initiate a new session.

Control Description

The organization requires users and devices to re-authenticate when [Assignment: organization-defined circumstances or situations requiring re-authentication].

Supplemental Guidance

In addition to the re-authentication requirements associated with session locks, organizations may require re-authentication of individuals and/or devices in other situations including, for example: (i) when authenticators change; (ii), when roles change; (iii) when security categories of information systems change; (iv), when the execution of privileged functions occurs; (v) after a fixed period of time; or (vi) periodically.

IR - Incident Response Control Family

Number	Control	Pivotal Application Service (PAS) Compliance
IR-1	INCIDENT RESPONSE POLICY AND PROCEDURES	Inherited
IR-2	INCIDENT RESPONSE TRAINING	Inherited
IR-3	INCIDENT RESPONSE TESTING	Inherited
IR-4	INCIDENT HANDLING	Inherited
IR-5	INCIDENT MONITORING	Inherited
IR-6	INCIDENT REPORTING	Inherited
IR-7	INCIDENT RESPONSE ASSISTANCE	Inherited and Compliant
IR-8	INCIDENT RESPONSE PLAN	Inherited
IR-9	INFORMATION SPILLAGE RESPONSE	P0, so not required for FISMA Moderate
IR-10	INTEGRATED INFORMATION SECURITY ANALYSIS TEAM	P0, so not required for FISMA Moderate

IR-1 INCIDENT RESPONSE POLICY AND PROCEDURES

PCF Compliance

All dash-1 requirements are the responsibility of the deployer. Pivotal may be able to provide guidance to customers who are creating or updating documentation, but this documentation is unique to the deployer's mission and business goals. All implied required satisfied. PCF features are sufficient to satisfy IR-1.

Control Description

The organization:

- a. 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
- b. Reviews and updates the current:
 1. Incident response policy [Assignment: organization-defined frequency]; and
 2. Incident response procedures [Assignment: organization-defined frequency].

Supplemental Guidance

This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the IR family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

IR-2 INCIDENT RESPONSE TRAINING

PCF Compliance

Compliance with this requirement is the responsibility of the PCF deployer.

Control Description

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

- a. Within [Assignment: organization-defined time period] of assuming an incident response role or responsibility;
- b. When required by information system changes; and
- c. [Assignment: organization-defined frequency] thereafter.

Supplemental Guidance

Incident response training provided by organizations is linked to the assigned roles and responsibilities of organizational personnel to ensure the appropriate content and level of detail is included in such training. For example, regular users may only need to know who to call or how to recognize an incident on the information system; system administrators may require additional training on how to handle/remediate incidents; and incident responders may receive more specific training on forensics, reporting, system recovery, and restoration. Incident response training includes user training in the identification and reporting of suspicious activities, both from external and internal sources.

IR-3 INCIDENT RESPONSE TESTING

PCF Compliance

Compliance with this requirement is the responsibility of the PCF deployer.

Control Description

The organization tests the incident response capability for the information system [Assignment: organization-defined frequency] using [Assignment: organization-defined tests] to determine the incident response effectiveness and documents the results.

Supplemental Guidance

Organizations test incident response capabilities to determine the overall effectiveness of the capabilities and to identify potential weaknesses or deficiencies. Incident response testing includes, for example, the use of checklists, walk-through or tabletop exercises, simulations (parallel/full interrupt), and comprehensive exercises. Incident response testing can also include a determination of the effects on organizational operations (e.g., reduction in mission capabilities), organizational assets, and individuals due to incident response.

IR-4 INCIDENT HANDLING

PCF Compliance

Compliance with this requirement is the responsibility of the PCF deployer.

Control Description

The organization:

- a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery;
- b. Coordinates incident handling activities with contingency planning activities; and
- c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implements the resulting changes accordingly.

Supplemental Guidance

Organizations recognize that incident response capability is dependent on the capabilities of organizational information systems and the mission/business processes being supported by those systems. Therefore, organizations consider incident response as part of the definition, design, and development of mission/business processes and information systems. Incident-related information can be obtained from a variety of sources including, for example, audit monitoring, network monitoring, physical access monitoring, user/administrator reports, and reported supply chain events. Effective incident handling capability includes coordination among many organizational entities including, for example, mission/business owners, information system owners, authorizing officials, human resources offices, physical and personnel security offices, legal departments, operations personnel, procurement offices, and the risk executive (function).

IR-5 INCIDENT MONITORING

PCF Compliance

Compliance with this requirement is the responsibility of the PCF deployer.

Control Description

The organization tracks and documents information system security incidents.

Supplemental Guidance

Documenting information system security incidents includes, for example, maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics, evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources including, for example, incident reports, incident response teams, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.

IR-6 INCIDENT REPORTING

PCF Compliance

Compliance with this requirement is the responsibility of the PCF deployer.

Control Description

The organization:

- a. Requires personnel to report suspected security incidents to the organizational incident response capability within [Assignment: organization-defined time period]; and
- b. Reports security incident information to [Assignment: organization-defined authorities].

Supplemental Guidance

The intent of this control is to address both specific incident reporting requirements within an organization and the formal incident reporting requirements for federal agencies and their subordinate organizations. Suspected security incidents include, for example, the receipt of suspicious email communications that can potentially contain malicious code. The types of security incidents reported, the content and timeliness of the reports, and the designated reporting authorities reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Current federal policy requires that all federal agencies (unless specifically exempted from such requirements) report security incidents to the United States Computer Emergency Readiness Team (US-CERT) within specified time frames designated in the US-CERT Concept of Operations for Federal Cyber Security Incident Handling.

IR-7 INCIDENT RESPONSE ASSISTANCE

PCF Compliance

Compliance with this requirement is the responsibility of the PCF deployer.

Pivotal provides the following incident response support resources:

- RSS feed of Pivotal vulnerability reports: <https://pivotal.io/security/rss>
 - Pivotal Product Vulnerability Reports, archived on the Pivotal Application Security Team website: <https://pivotal.io/security>
 - Pivotal Support website and assistance request system: <https://support.pivotal.io>
 - Pivotal Application Security Team email: security@pivotal.io
-

Control Description

Incident response support resources provided by organizations include, for example, help desks, assistance groups, and access to forensics services, when required.

Supplemental Guidance

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-8 INCIDENT RESPONSE PLAN

PCF Compliance

Compliance with this requirement is the responsibility of the PCF deployer.

Control Description

The organization:

- a. 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];
- b. Distributes copies of the incident response plan to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements];
- c. Reviews the incident response plan [Assignment: organization-defined frequency];
- d. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing;
- e. Communicates incident response plan changes to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; and
- f. Protects the incident response plan from unauthorized disclosure and modification.

Supplemental Guidance

It is important that organizations develop and implement a coordinated approach to incident response. Organizational missions, business functions, strategies, goals, and objectives for incident response help to determine the structure of incident response capabilities. As part of a comprehensive incident response capability, organizations consider the coordination and sharing of information with external organizations, including, for example, external service providers and organizations involved in the supply chain for organizational information systems.

IR-9 INFORMATION SPILLAGE RESPONSE

PCF Compliance

P0, so not required for [FISMA](#) Moderate.

Control Description

The organization responds to information spills by:

- a. Identifying the specific information involved in the information system contamination;
- b. Alerting [Assignment: organization-defined personnel or roles] of the information spill using a method of communication not associated with the spill;
- c. Isolating the contaminated information system or system component;
- d. Eradicating the information from the contaminated information system or component;
- e. Identifying other information systems or system components that may have been subsequently contaminated; and
- f. Performing other [Assignment: organization-defined actions].

Supplemental Guidance

Information spillage refers to instances where either classified or sensitive information is inadvertently placed on information systems that are not authorized to process such information. Such information spills often occur when information that is initially thought to be of lower sensitivity is transmitted to an information system and then is subsequently determined to be of higher sensitivity. At that point, corrective action is required. The nature of the organizational response is generally based upon the degree of sensitivity of the spilled information (e.g., security category or classification level), the security capabilities of the information system, the specific nature of contaminated storage media, and the access authorizations (e.g., security clearances) of individuals with authorized access to the contaminated system. The methods used to communicate information about the spill after the fact do not involve methods directly associated with the actual spill to minimize the risk of further spreading the contamination before such contamination is isolated and eradicated.

IR-10 INTEGRATED INFORMATION SECURITY ANALYSIS TEAM

PCF Compliance

PO, so not required for [FISMA](#) [Moderate](#).

Control Description

The organization establishes an integrated team of forensic/malicious code analysts, tool developers, and real-time operations personnel.

Supplemental Guidance

Having an integrated team for incident response facilitates information sharing. Such capability allows organizational personnel, including developers, implementers, and operators, to leverage the team knowledge of the threat in order to implement defensive measures that will enable organizations to deter intrusions more effectively. Moreover, it promotes the rapid detection of intrusions, development of appropriate mitigations, and the deployment of effective defensive measures. For example, when an intrusion is detected, the integrated security analysis team can rapidly develop an appropriate response for operators to implement, correlate the new incident with information on past intrusions, and augment ongoing intelligence development. This enables the team to identify adversary TTPs that are linked to the operations tempo or to specific missions/business functions, and to define responsive actions in a way that does not disrupt the mission/business operations. Ideally, information security analysis teams are distributed within organizations to make the capability more resilient.

MA - Maintenance Control Family

Number	Control	Pivotal Application Service (PAS) Compliance
MA-1	SYSTEM MAINTENANCE POLICY AND PROCEDURES	Deployer responsibility
MA-2	CONTROLLED MAINTENANCE	Deployer responsibility
MA-3	MAINTENANCE TOOLS	Deployer responsibility
MA-4	NONLOCAL MAINTENANCE	Deployer responsibility
MA-5	MAINTENANCE PERSONNEL	Deployer responsibility
MA-6	TIMELY MAINTENANCE	Deployer responsibility

MA-1 SYSTEM MAINTENANCE POLICY AND PROCEDURES

PCF Compliance

All xx-1 requirements are the responsibility of the deployer. The PCF product feature set is sufficient to satisfy the technical requirements implied in MA-1. Pivotal may be able to provide guidance to customers who are creating or updating documentation, but this documentation is unique to the deployer's mission and business goals.

Control Description

The organization:

- a. 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
- b. Reviews and updates the current:
 1. System maintenance policy [Assignment: organization-defined frequency]; and
 2. System maintenance procedures [Assignment: organization-defined frequency].

Supplemental Guidance

This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the MA family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

MA-2 CONTROLLED MAINTENANCE

PCF Compliance

Regular maintenance of a PAS deployment is accomplished using BOSH and Ops Manager. Approval for maintenance activities and the associated record-keeping requirements are the responsibility of the deployer. Handling procedures for proper custody or hardware will vary based on the IaaS, and are the responsibility of the deployer. Appropriate procedures for sanitization of persistent storage volumes are IaaS-specific, and will vary based on, e.g., whether the PAS deployment is part of a public or private cloud deployment.

Control Description

The organization:

- a. 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;
- b. 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;
- c. 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;
- d. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs;
- e. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and
- f. Includes [Assignment: organization-defined maintenance-related information] in organizational maintenance records.

Supplemental Guidance

This control addresses the information security aspects of the information system maintenance program and applies to all types of maintenance to any system component (including applications) conducted by any local or nonlocal entity (e.g., in-contract, warranty, in-house, software maintenance agreement). System maintenance also includes those components not directly associated with information processing and/or data/information retention such as scanners, copiers, and printers. Information necessary for creating effective maintenance records includes, for example: (i) date and time of maintenance; (ii) name of individuals or group performing the maintenance; (iii) name of escort, if necessary; (iv) a description of the maintenance performed; and (v) information system components/equipment removed or replaced (including identification numbers, if applicable). The level of detail included in maintenance records can be informed by the security categories of organizational information systems. Organizations consider supply chain issues associated with replacement components for information systems.

MA-3 MAINTENANCE TOOLS

PCF Compliance

Compliance with the requirements defined in this control are a deployer responsibility.

Control Description

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

Supplemental Guidance

This control addresses security-related issues associated with maintenance tools used specifically for diagnostic and repair actions on organizational information systems. Maintenance tools can include hardware, software, and firmware items. Maintenance tools are potential vehicles for transporting malicious code, either intentionally or unintentionally, into a facility and subsequently into organizational information systems. Maintenance tools can include, for example, hardware/software diagnostic test equipment and hardware/software packet sniffers. This control does not cover hardware/software components that may support information system maintenance, yet are a part of the system, for example, the software implementing “ping,” “ls,” “ipconfig,” or the hardware and software implementing the monitoring port of an Ethernet switch.

MA-4 NONLOCAL MAINTENANCE

PCF Compliance

Compliance with the requirements defined in this control are a deployer responsibility.

Nonlocal maintenance is interpreted to mean performing remote support via an authenticated network connection. Operators have the option to enable SSH login to PAS VMs using either the BOSH CLI, and/or via any standard SSH client.

Control Description

The organization:

- a. Approves and monitors nonlocal maintenance and diagnostic activities;
- b. 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;
- c. Employs strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions;
- d. Maintains records for nonlocal maintenance and diagnostic activities; and
- e. Terminates session and network connections when nonlocal maintenance is completed.

Supplemental Guidance

Nonlocal maintenance and diagnostic activities are those activities conducted by individuals communicating through a network, either an external network (e.g., the Internet) or an internal network. Local maintenance and diagnostic activities are those activities carried out by individuals physically present at the information system or information system component and not communicating across a network connection. Authentication techniques used in the establishment of nonlocal maintenance and diagnostic sessions reflect the network access requirements in IA-2. Typically, strong authentication requires authenticators that are resistant to replay attacks and employ multifactor authentication. Strong authenticators include, for example, PKI where certificates are stored on a token protected by a password, passphrase, or biometric. Enforcing requirements in MA-4 is accomplished in part by other controls.

MA-5 MAINTENANCE PERSONNEL

PCF Compliance

Compliance with the requirements defined in this control are a deployer responsibility.

Control Description

The organization:

- a. Establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel;
- b. Ensures that non-escorted personnel performing maintenance on the information system have required access authorizations; and
- c. 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.

Supplemental Guidance

This control applies to individuals performing hardware or software maintenance on organizational information systems, while PE-2 addresses physical access for individuals whose maintenance duties place them within the physical protection perimeter of the systems (e.g., custodial staff, physical plant maintenance personnel). Technical competence of supervising individuals relates to the maintenance performed on the information systems while having required access authorizations refers to maintenance on and near the systems. Individuals not previously identified as authorized maintenance personnel, such as information technology manufacturers, vendors, systems integrators, and consultants, may require privileged access to organizational information systems, for example, when required to conduct maintenance activities with little or no notice. Based on organizational assessments of risk, organizations may issue temporary credentials to these individuals. Temporary credentials may be for one-time use or for very limited time periods.

MA-6 TIMELY MAINTENANCE

PCF Compliance

Compliance with the requirements defined in this control are a deployer responsibility.

The PCF platform provides the organization with a high availability environment, such that an unplanned maintenance event due to hardware or software failure should not result in any application down time. For example, when supported by the underlying IaaS, the PCF deployment may be operated across multiple availability zones, in order to protect against loss of a specific geographic location. In the event that spare parts are needed to restore service at a specific geographic location, the applications hosted on PCF should remain available via, e.g., another availability zone.

Control Description

The organization obtains maintenance support and/or spare parts for [Assignment: organization-defined information system components] within [Assignment: organization-defined time period] of failure.

Supplemental Guidance

Organizations specify the information system components that result in increased risk to organizational operations and assets, individuals, other organizations, or the Nation when the functionality provided by those components is not operational. Organizational actions to obtain maintenance support typically include having appropriate contracts in place.

MP - Media Protection Control Family

Number	Control	Pivotal Application Service (PAS) Compliance
MP-1	MEDIA PROTECTION POLICY AND PROCEDURES	Inherited
MP-2	MEDIA ACCESS	Inherited
MP-3	MEDIA MARKING	Inherited
MP-4	MEDIA STORAGE	Inherited
MP-5	MEDIA TRANSPORT	Inherited
MP-6	MEDIA SANITIZATION	Inherited
MP-7	MEDIA USE	Inherited
MP-8	MEDIA DOWNGRADING	P0, so not required for FISMA Moderate

MP-1 MEDIA PROTECTION POLICY AND PROCEDURES

PCF Compliance

All dash-1 requirements are the responsibility of the deployer. Pivotal may be able to provide guidance to customers who are creating or updating documentation, but this documentation is unique to the deployer's mission and business goals. All implied requirements are satisfied. PCF features are sufficient to satisfy MP-1.

Control Description

The organization:

- a. 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
- b. Reviews and updates the current:
 1. Media protection policy [Assignment: organization-defined frequency]; and
 2. Media protection procedures [Assignment: organization-defined frequency].

Supplemental Guidance

This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the MP family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

MP-2 MEDIA ACCESS

PCF Compliance

Compliance with this requirement is the responsibility of the PCF deployer.

Control Description

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

Supplemental Guidance

Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. Restricting non-digital media access includes, for example, denying access to patient medical records in a community hospital unless the individuals seeking access to such records are authorized healthcare providers. Restricting access to digital media includes, for example, limiting access to design specifications stored on compact disks in the media library to the project leader and the individuals on the development team.

MP-3 MEDIA MARKING

PCF Compliance

Compliance with this requirement is the responsibility of the PCF deployer.

Control Description

The organization:

- a. Marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and
- b. Exempts [Assignment: organization-defined types of information system media] from marking as long as the media remain within [Assignment: organization-defined controlled areas].

Supplemental Guidance

The term security marking refers to the application/use of human-readable security attributes. The term security labeling refers to the application/use of security attributes with regard to internal data structures within information systems (see AC-16). Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. Security marking is generally not required for media containing information determined by organizations to be in the public domain or to be publicly releasable. However, some organizations may require markings for public information indicating that the information is publicly releasable. Marking of information system media reflects applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

MP-4 MEDIA STORAGE

PCF Compliance

Compliance with this requirement is the responsibility of the PCF deployer.

Control Description

The organization:

- a. Physically controls and securely stores [Assignment: organization-defined types of digital and/or non-digital media] within [Assignment: organization-defined controlled areas]; and
- b. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

Supplemental Guidance

Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. Physically controlling information system media includes, for example, conducting inventories, ensuring procedures are in place to allow individuals to check out and return media to the media library, and maintaining accountability for all stored media. Secure storage includes, for example, a locked drawer, desk, or cabinet, or a controlled media library. The type of media storage is commensurate with the security category and/or classification of the information residing on the media. Controlled areas are areas for which organizations provide sufficient physical and procedural safeguards to meet the requirements established for protecting information and/or information systems. For media containing information determined by organizations to be in the public domain, to be publicly releasable, or to have limited or no adverse impact on organizations or individuals if accessed by other than authorized personnel, fewer safeguards may be needed. In these situations, physical access controls provide adequate protection.

MP-5 MEDIA TRANSPORT

PCF Compliance

Compliance with this requirement is the responsibility of the PCF deployer.

Control Description

The organization:

- a. Protects and controls [Assignment: organization-defined types of information system media] during transport outside of controlled areas using [Assignment: organization-defined security safeguards];
- b. Maintains accountability for information system media during transport outside of controlled areas;
- c. Documents activities associated with the transport of information system media; and
- d. Restricts the activities associated with the transport of information system media to authorized personnel.

Supplemental Guidance

Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. This control also applies to mobile devices with information storage capability (e.g., smart phones, tablets, E-readers), that are transported outside of controlled areas. Controlled areas are areas or spaces for which organizations provide sufficient physical and/or procedural safeguards to meet the requirements established for protecting information and/or information systems. Physical and technical safeguards for media are commensurate with the security category or classification of the information residing on the media. Safeguards to protect media during transport include, for example, locked containers and cryptography. Cryptographic mechanisms can provide confidentiality and integrity protections depending upon the mechanisms used. Activities associated with transport include the actual transport as well as those activities such as releasing media for transport and ensuring that media enters the appropriate transport processes. For the actual transport, authorized transport and courier personnel may include individuals from outside the organization (e.g., U.S. Postal Service or a commercial transport or delivery service). Maintaining accountability of media during transport includes, for example, restricting transport activities to authorized personnel, and tracking and/or obtaining explicit records of transport activities as the media moves through the transportation system to prevent and detect loss, destruction, or tampering. Organizations establish documentation requirements for activities associated with the transport of information system media in accordance with organizational assessments of risk to include the flexibility to define different record-keeping methods for the different types of media transport as part of an overall system of transport-related records.

MP-6 MEDIA SANITIZATION

PCF Compliance

Compliance with this requirement is the responsibility of the PCF deployer.

The ability to erase residual data on boot, ephemeral, or persistent volumes after they are decommissioned from a PCF deployment inherits from and depends on PCF's underlying infrastructure.

Control Description

The organization:

- a. 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
- b. Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

Supplemental Guidance

This control applies to all information system media, both digital and non-digital, subject to disposal or reuse, whether or not the media is considered removable. Examples include media found in scanners, copiers, printers, notebook computers, workstations, network components, and mobile devices. The sanitization process removes information from the media such that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, cryptographic erase, and destruction, prevent the disclosure of information to unauthorized individuals when such media is reused or released for disposal. Organizations determine the appropriate sanitization methods recognizing that destruction is sometimes necessary when other methods cannot be applied to media requiring sanitization. Organizations use discretion on the employment of approved sanitization techniques and procedures for media containing information deemed to be in the public domain or publicly releasable, or deemed to have no adverse impact on organizations or individuals if released for reuse or disposal. Sanitization of non-digital media includes, for example, removing a classified appendix from an otherwise unclassified document, or redacting selected sections or words from a document by obscuring the redacted sections/words in a manner equivalent in effectiveness to removing them from the document. NSA standards and policies control the sanitization process for media containing classified information.

MP-7 MEDIA USE

PCF Compliance

Compliance with this requirement is the responsibility of the PCF deployer.

Control Description

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].

Supplemental Guidance

Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. This control also applies to mobile devices with information storage capability (e.g., smart phones, tablets, E-readers). In contrast to MP-2, which restricts user access to media, this control restricts the use of certain types of media on information systems, for example, restricting/prohibiting the use of flash drives or external hard disk drives. Organizations can employ technical and nontechnical safeguards (e.g., policies, procedures, rules of behavior) to restrict the use of information system media. Organizations may restrict the use of portable storage devices, for example, by using physical cages on workstations to prohibit access to certain external ports, or disabling/removing the ability to insert, read or write to such devices. Organizations may also limit the use of portable storage devices to only approved devices including, for example, devices provided by the organization, devices provided by other approved organizations, and devices that are not personally owned. Finally, organizations may restrict the use of portable storage devices based on the type of device, for example, prohibiting the use of writeable, portable storage devices, and implementing this restriction by disabling or removing the capability to write to such devices.

MP-8 MEDIA DOWNGRADING

PCF Compliance

Compliance with this requirement is the responsibility of the PCF deployer.

Control Description

The organization:

- a. Establishes [Assignment: organization-defined information system media downgrading process] that includes employing downgrading mechanisms with [Assignment: organization-defined strength and integrity];
- b. Ensures that the information system media downgrading process is commensurate with the security category and/or classification level of the information to be removed and the access authorizations of the potential recipients of the downgraded information;
- c. Identifies [Assignment: organization-defined information system media requiring downgrading]; and
- d. Downgrades the identified information system media using the established process.

Supplemental Guidance

This control applies to all information system media, digital and non-digital, subject to release outside of the organization, whether or not the media is considered removable. The downgrading process, when applied to system media, removes information from the media, typically by security category or classification level, such that the information cannot be retrieved or reconstructed. Downgrading of media includes redacting information to enable wider release and distribution. Downgrading of media also ensures that empty space on the media (e.g., slack space within files) is devoid of information.

Personnel Security Control Family

Number	Control	Pivotal Application Service (PAS) Compliance
PS-1	PERSONNEL SECURITY POLICY AND PROCEDURES	Deployer responsibility
PS-2	POSITION RISK DESIGNATION	Deployer responsibility
PS-3	PERSONNEL SCREENING	Deployer responsibility
PS-4	PERSONNEL TERMINATION	Deployer responsibility
PS-5	PERSONNEL TRANSFER	Deployer responsibility
PS-6	ACCESS AGREEMENTS	Deployer responsibility
PS-7	THIRD-PARTY PERSONNEL SECURITY	Deployer responsibility
PS-8	PERSONNEL SANCTIONS	Deployer responsibility

PS-1 PERSONNEL SECURITY POLICY AND PROCEDURES

PCF Compliance

All xx-1 requirements are the responsibility of the deployer. The PCF product feature set is sufficient to satisfy the technical requirements implied in PS-1. Pivotal may be able to provide guidance to customers who are creating or updating documentation, but this documentation is unique to the deployer's mission and business goals.

Control Description

The organization:

- a. 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
- b. Reviews and updates the current:
 1. Personnel security policy [Assignment: organization-defined frequency]; and
 2. Personnel security procedures [Assignment: organization-defined frequency].

Supplemental Guidance

This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the PS family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

PS-2 POSITION RISK DESIGNATION

PCF Compliance

Compliance with the requirements defined in this control are a deployer responsibility.

Control Description

The organization:

- a. Assigns a risk designation to all organizational positions;
- b. Establishes screening criteria for individuals filling those positions; and
- c. Reviews and updates position risk designations [Assignment: organization-defined frequency].

Supplemental Guidance

Position risk designations reflect Office of Personnel Management policy and guidance. Risk designations can guide and inform the types of authorizations individuals receive when accessing organizational information and information systems. Position screening criteria include explicit information security role appointment requirements (e.g., training, security clearances).

PS-3 PERSONNEL SCREENING

PCF Compliance

Compliance with the requirements defined in this control are a deployer responsibility.

Control Description

The organization:

- a. Screens individuals prior to authorizing access to the information system; and
- b. Rescreens individuals according to [Assignment: organization-defined conditions requiring rescreening and, where rescreening is so indicated, the frequency of such rescreening].

Supplemental Guidance

Personnel screening and rescreening activities reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, guidance, and specific criteria established for the risk designations of assigned positions. Organizations may define different rescreening conditions and frequencies for personnel accessing information systems based on types of information processed, stored, or transmitted by the systems.

PS-4 PERSONNEL TERMINATION

PCF Compliance

Compliance with the requirements defined in this control are a deployer responsibility.

Control Description

The organization, upon termination of individual employment:

- a. Disables information system access within [Assignment: organization-defined time period];
- b. Terminates/revokes any authenticators/credentials associated with the individual;
- c. Conducts exit interviews that include a discussion of [Assignment: organization-defined information security topics];
- d. Retrieves all security-related organizational information system-related property;
- e. Retains access to organizational information and information systems formerly controlled by terminated individual; and
- f. Notifies [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period].

Supplemental Guidance

Information system-related property includes, for example, hardware authentication tokens, system administration technical manuals, keys, identification cards, and building passes. Exit interviews ensure that terminated individuals understand the security constraints imposed by being former employees and that proper accountability is achieved for information system-related property. Security topics of interest at exit interviews can include, for example, reminding terminated individuals of nondisclosure agreements and potential limitations on future employment. Exit interviews may not be possible for some terminated individuals, for example, in cases related to job abandonment, illnesses, and nonavailability of supervisors. Exit interviews are important for individuals with security clearances. Timely execution of termination actions is essential for individuals terminated for cause. In certain situations, organizations consider disabling the information system accounts of individuals that are being terminated prior to the individuals being notified.

PS-5 PERSONNEL TRANSFER

PCF Compliance

Compliance with the requirements defined in this control are a deployer responsibility.

Control Description

The organization:

- a. 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;
- b. Initiates [Assignment: organization-defined transfer or reassignment actions] within [Assignment: organization-defined time period following the formal transfer action];
- c. Modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and
- d. Notifies [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period].

Supplemental Guidance

This control applies when reassignments or transfers of individuals are permanent or of such extended durations as to make the actions warranted. Organizations define actions appropriate for the types of reassignments or transfers, whether permanent or extended. Actions that may be required for personnel transfers or reassignments to other positions within organizations include, for example: (i) returning old and issuing new keys, identification cards, and building passes; (ii) closing information system accounts and establishing new accounts; (iii) changing information system access authorizations (i.e., privileges); and (iv) providing for access to official records to which individuals had access at previous work locations and in previous information system accounts.

PS-6 ACCESS AGREEMENTS

PCF Compliance

Compliance with the requirements defined in this control are a deployer responsibility.

Control Description

The organization:

- a. Develops and documents access agreements for organizational information systems;
- b. Reviews and updates the access agreements [Assignment: organization-defined frequency]; and
- c. 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 [Assignment: organization-defined frequency].

Supplemental Guidance

Access agreements include, for example, nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. Signed access agreements include an acknowledgement that individuals have read, understand, and agree to abide by the constraints associated with organizational information systems to which access is authorized. Organizations can use electronic signatures to acknowledge access agreements unless specifically prohibited by organizational policy.

PS-7 THIRD-PARTY PERSONNEL SECURITY

PCF Compliance

Compliance with the requirements defined in this control are a deployer responsibility.

Control Description

The organization:

- a. Establishes personnel security requirements including security roles and responsibilities for third-party providers;
- b. Requires third-party providers to comply with personnel security policies and procedures established by the organization;
- c. Documents personnel security requirements;
- d. 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 [Assignment: organization-defined time period]; and
- e. Monitors provider compliance.

Supplemental Guidance

Third-party providers include, for example, service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, and network and security management. Organizations explicitly include personnel security requirements in acquisition-related documents. Third-party providers may have personnel working at organizational facilities with credentials, badges, or information system privileges issued by organizations. Notifications of third-party personnel changes ensure appropriate termination of privileges and credentials. Organizations define the transfers and terminations deemed reportable by security-related characteristics that include, for example, functions, roles, and nature of credentials/privileges associated with individuals transferred or terminated.

PS-8 PERSONNEL SANCTIONS

PCF Compliance

Compliance with the requirements defined in this control are a deployer responsibility.

Control Description

The organization:

- a. Employs a formal sanctions process for individuals failing to comply with established information security policies and procedures; and
- b. 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.

Supplemental Guidance

Organizational sanctions processes reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Sanctions processes are described in access agreements and can be included as part of general personnel policies and procedures for organizations. Organizations consult with the Office of the General Counsel regarding matters of employee sanctions.

PE - Physical and Environmental Protection Control Family

Number	Control	Pivotal Application Service (PAS) Compliance
PE-1	PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES	Inherited
PE-2	PHYSICAL ACCESS AUTHORIZATIONS	Inherited
PE-3	PHYSICAL ACCESS CONTROL	Inherited
PE-4	ACCESS CONTROL FOR TRANSMISSION MEDIUM	Inherited
PE-5	ACCESS CONTROL FOR OUTPUT DEVICES	Inherited
PE-6	MONITORING PHYSICAL ACCESS	Inherited
PE-7	VISITOR CONTROL	Inherited
PE-8	VISITOR ACCESS RECORDS	Inherited
PE-9	POWER EQUIPMENT AND CABLING	Inherited
PE-10	EMERGENCY SHUTOFF	Inherited
PE-11	EMERGENCY POWER	Inherited
PE-12	EMERGENCY LIGHTING	Inherited
PE-13	FIRE PROTECTION	Inherited
PE-14	TEMPERATURE AND HUMIDITY CONTROLS	Inherited
PE-15	WATER DAMAGE PROTECTION	Inherited
PE-16	DELIVERY AND REMOVAL	Inherited
PE-17	ALTERNATE WORK SITE	Inherited
PE-18	LOCATION OF INFORMATION SYSTEM COMPONENTS	Not required for FISMA Moderate
PE-19	INFORMATION LEAKAGE	P0, so not required for FISMA Moderate
PE-20	ASSET MONITORING AND TRACKING	P0, so not required for FISMA Moderate

PE-1 PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES

PCF Compliance

All dash-1 requirements are the responsibility of the deployer. Pivotal may be able to provide guidance to customers who are creating or updating documentation, but this documentation is unique to the deployer's mission and business goals. All implied requirements are satisfied. PCF features are sufficient to satisfy PE-1.

Control Description

The organization:

- a. 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
- b. Reviews and updates the current:
 - 1. Physical and environmental protection policy [Assignment: organization-defined frequency]; and
 - 2. Physical and environmental protection procedures [Assignment: organization-defined frequency].

Supplemental Guidance

This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the PE family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

PE-2 PHYSICAL ACCESS AUTHORIZATIONS

PCF Compliance

Compliance with this requirement is the responsibility of the PCF deployer.

Control Description

The organization:

- a. Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides;
- b. Issues authorization credentials for facility access;
- c. Reviews the access list detailing authorized facility access by individuals [Assignment: organization-defined frequency]; and
- d. Removes individuals from the facility access list when access is no longer required.

Supplemental Guidance

This control applies to organizational employees and visitors. Individuals (e.g., employees, contractors, and others) with permanent physical access authorization credentials are not considered visitors. Authorization credentials include, for example, badges, identification cards, and smart cards. Organizations determine the strength of authorization credentials needed (including level of forge-proof badges, smart cards, or identification cards) consistent with federal standards, policies, and procedures. This control only applies to areas within facilities that have not been designated as publicly accessible.

PE-3 PHYSICAL ACCESS CONTROL

PCF Compliance

Compliance with this requirement is the responsibility of the PCF deployer.

Control Description

The organization:

- a. 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 [Selection (one or more): [Assignment: organization-defined physical access control systems/devices]; guards];
- b. Maintains physical access audit logs for [Assignment: organization-defined entry/exit points];
- c. Provides [Assignment: organization-defined security safeguards] to control access to areas within the facility officially designated as publicly accessible;
- d. Escorts visitors and monitors visitor activity [Assignment: organization-defined circumstances requiring visitor escorts and monitoring];
- e. Secures keys, combinations, and other physical access devices;
- f. Inventories [Assignment: organization-defined physical access devices] every [Assignment: organization-defined frequency]; and
- g. Changes combinations and keys [Assignment: organization-defined frequency] and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.

Supplemental Guidance

This control applies to organizational employees and visitors. Individuals (e.g., employees, contractors, and others) with permanent physical access authorization credentials are not considered visitors. Organizations determine the types of facility guards needed including, for example, professional physical security staff or other personnel such as administrative staff or information system users. Physical access devices include, for example, keys, locks, combinations, and card readers. Safeguards for publicly accessible areas within organizational facilities include, for example, cameras, monitoring by guards, and isolating selected information systems and/or system components in secured areas. Physical access control systems comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. The Federal Identity, Credential, and Access Management Program provides implementation guidance for identity, credential, and access management capabilities for physical access control systems. Organizations have flexibility in the types of audit logs employed. Audit logs can be procedural (e.g., a written log of individuals accessing the facility and when such access occurred), automated (e.g., capturing ID provided by a PIV card), or some combination thereof. Physical access points can include facility access points, interior access points to information systems and/or components requiring supplemental access controls, or both. Components of organizational information systems (e.g., workstations, terminals) may be located in areas designated as publicly accessible with organizations safeguarding access to such devices.

PE-4 ACCESS CONTROL FOR TRANSMISSION MEDIUM

PCF Compliance

Compliance with this requirement is the responsibility of the PCF deployer.

Control Description

The organization controls physical access to [Assignment: organization-defined information system distribution and transmission lines] within organizational facilities using [Assignment: organization-defined security safeguards].

Supplemental Guidance

Physical security safeguards applied to information system distribution and transmission lines help to prevent accidental damage, disruption, and physical tampering. In addition, physical safeguards may be necessary to help prevent eavesdropping or in transit modification of unencrypted transmissions. Security safeguards to control physical access to system distribution and transmission lines include, for example: (i) locked wiring closets; (ii) disconnected or locked spare jacks; and/or (iii) protection of cabling by conduit or cable trays.

PE-5 ACCESS CONTROL FOR OUTPUT DEVICES

PCF Compliance

Compliance with this requirement is the responsibility of the PCF deployer.

Control Description

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

Supplemental Guidance

Controlling physical access to output devices includes, for example, placing output devices in locked rooms or other secured areas and allowing access to authorized individuals only, and placing output devices in locations that can be monitored by organizational personnel. Monitors, printers, copiers, scanners, facsimile machines, and audio devices are examples of information system output devices.

PE-6 MONITORING PHYSICAL ACCESS

PCF Compliance

Compliance with this requirement is the responsibility of the PCF deployer.

Control Description

The organization:

- a. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents;
- b. Reviews physical access logs [Assignment: organization-defined frequency] and upon occurrence of [Assignment: organization-defined events or potential indications of events]; and
- c. Coordinates results of reviews and investigations with the organizational incident response capability.

Supplemental Guidance

Organizational incident response capabilities include investigations of and responses to detected physical security incidents. Security incidents include, for example, apparent security violations or suspicious physical access activities. Suspicious physical access activities include, for example: (i) accesses outside of normal work hours; (ii) repeated accesses to areas not normally accessed; (iii) accesses for unusual lengths of time; and (iv) out-of-sequence accesses.

PE-7 VISITOR CONTROL

Control Description

[Withdrawn: Incorporated into PE-2 and PE-3].

Supplemental Guidance

PE-8 VISITOR ACCESS RECORDS

PCF Compliance

Compliance with this requirement is the responsibility of the PCF deployer.

Control Description

The organization:

- a. Maintains visitor access records to the facility where the information system resides for [Assignment: organization-defined time period]; and
- b. Reviews visitor access records [Assignment: organization-defined frequency].

Supplemental Guidance

Visitor access records include, for example, names and organizations of persons visiting, visitor signatures, forms of identification, dates of access, entry and departure times, purposes of visits, and names and organizations of persons visited. Visitor access records are not required for publicly accessible areas.

PE-9 POWER EQUIPMENT AND CABLING

PCF Compliance

Compliance with this requirement is the responsibility of the PCF deployer.

Control Description

The organization protects power equipment and power cabling for the information system from damage and destruction.

Supplemental Guidance

Organizations determine the types of protection necessary for power equipment and cabling employed at different locations both internal and external to organizational facilities and environments of operation. This includes, for example, generators and power cabling outside of buildings, internal cabling and uninterruptable power sources within an office or data center, and power sources for self-contained entities such as vehicles and satellites.

PE-10 EMERGENCY SHUTOFF

PCF Compliance

Compliance with this requirement is the responsibility of the PCF deployer.

Control Description

The organization:

- a. Provides the capability of shutting off power to the information system or individual system components in emergency situations;
- b. 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
- c. Protects emergency power shutoff capability from unauthorized activation.

Supplemental Guidance

This control applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms.

PE-11 EMERGENCY POWER

PCF Compliance

Compliance with this requirement is the responsibility of the PCF deployer.

Control Description

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.

Supplemental Guidance

PE-12 EMERGENCY LIGHTING

PCF Compliance

Compliance with this requirement is the responsibility of the PCF deployer.

Control Description

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.

Supplemental Guidance

This control applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms.

PE-13 FIRE PROTECTION

PCF Compliance

Compliance with this requirement is the responsibility of the PCF deployer.

Control Description

The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.

Supplemental Guidance

This control applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms. Fire suppression and detection devices/systems include, for example, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors.

PE-14 TEMPERATURE AND HUMIDITY CONTROLS

PCF Compliance

Compliance with this requirement is the responsibility of the PCF deployer.

Control Description

The organization:

- a. Maintains temperature and humidity levels within the facility where the information system resides at [Assignment: organization-defined acceptable levels]; and
- b. Monitors temperature and humidity levels [Assignment: organization-defined frequency].

Supplemental Guidance

This control applies primarily to facilities containing concentrations of information system resources, for example, data centers, server rooms, and mainframe computer rooms.

PE-15 WATER DAMAGE PROTECTION

PCF Compliance

Compliance with this requirement is the responsibility of the PCF deployer.

Control Description

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.

Supplemental Guidance

This control applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms. Isolation valves can be employed in addition to or in lieu of master shutoff valves to shut off water supplies in specific areas of concern, without affecting entire organizations.

PE-16 DELIVERY AND REMOVAL

PCF Compliance

Compliance with this requirement is the responsibility of the PCF deployer.

Control Description

The organization authorizes, monitors, and controls [Assignment: organization-defined types of information system components] entering and exiting the facility and maintains records of those items.

Supplemental Guidance

Effectively enforcing authorizations for entry and exit of information system components may require restricting access to delivery areas and possibly isolating the areas from the information system and media libraries.

PE-17 ALTERNATE WORK SITE

PCF Compliance

Compliance with this requirement is the responsibility of the PCF deployer.

Control Description

The organization:

- a. Employs [Assignment: organization-defined security controls] at alternate work sites;
- b. Assesses as feasible, the effectiveness of security controls at alternate work sites; and
- c. Provides a means for employees to communicate with information security personnel in case of security incidents or problems.

Supplemental Guidance

Alternate work sites may include, for example, government facilities or private residences of employees. While commonly distinct from alternative processing sites, alternate work sites may provide readily available alternate locations as part of contingency operations. Organizations may define different sets of security controls for specific alternate work sites or types of sites depending on the work-related activities conducted at those sites. This control supports the contingency planning activities of organizations and the federal telework initiative.

PE-18 LOCATION OF INFORMATION SYSTEM COMPONENTS

PCF Compliance

Compliance with this requirement is the responsibility of the PCF deployer.

Control Description

The organization positions information system components within the facility to minimize potential damage from [Assignment: organization-defined physical and environmental hazards] and to minimize the opportunity for unauthorized access.

Supplemental Guidance

Physical and environmental hazards include, for example, flooding, fire, tornados, earthquakes, hurricanes, acts of terrorism, vandalism, electromagnetic pulse, electrical interference, and other forms of incoming electromagnetic radiation. In addition, organizations consider the location of physical entry points where unauthorized individuals, while not being granted access, might nonetheless be in close proximity to information systems and therefore increase the potential for unauthorized access to organizational communications (e.g., through the use of wireless sniffers or microphones).

PE-19 INFORMATION LEAKAGE

PCF Compliance

Compliance with this requirement is the responsibility of the PCF deployer.

Control Description

The organization protects the information system from information leakage due to electromagnetic signals emanations.

Supplemental Guidance

Information leakage is the intentional or unintentional release of information to an untrusted environment from electromagnetic signals emanations. Security categories or classifications of information systems (with respect to confidentiality) and organizational security policies guide the selection of security controls employed to protect systems against information leakage due to electromagnetic signals emanations.

PE-20 ASSET MONITORING AND TRACKING

PCF Compliance

Compliance with this requirement is the responsibility of the PCF deployer.

Control Description

The organization:

- a. Employs [Assignment: organization-defined asset location technologies] to track and monitor the location and movement of [Assignment: organization-defined assets] within [Assignment: organization-defined controlled areas]; and
- b. Ensures that asset location technologies are employed in accordance with applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance.

Supplemental Guidance

Asset location technologies can help organizations ensure that critical assets such as vehicles or essential information system components remain in authorized locations. Organizations consult with the Office of the General Counsel and the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) regarding the deployment and use of asset location technologies to address potential privacy concerns.

PL - Planning Control Family

Number	Control	Pivotal Application Service (PAS) Compliance
PL-1	SECURITY PLANNING POLICY AND PROCEDURES	Deployer responsibility
PL-2	SYSTEM SECURITY PLAN	Deployer responsibility
PL-3	SYSTEM SECURITY PLAN UPDATE	Deployer responsibility
PL-4	RULES OF BEHAVIOR	Deployer responsibility
PL-5	PRIVACY IMPACT ASSESSMENT	Deployer responsibility
PL-6	SECURITY-RELATED ACTIVITY PLANNING	Deployer responsibility
PL-7	SECURITY CONCEPT OF OPERATIONS	Deployer responsibility
PL-8	INFORMATION SECURITY ARCHITECTURE	Deployer responsibility
PL-9	CENTRAL MANAGEMENT	Deployer responsibility

PL-1 SECURITY PLANNING POLICY AND PROCEDURES

PCF Compliance

All requirements are the responsibility of the deployer. The PCF product feature set is sufficient to satisfy the technical requirements implied in PL-1. Pivotal may be able to provide guidance to customers who are creating or updating documentation, but this documentation is unique to the deployer's mission and business goals.

Control Description

The organization:

- a. 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
- b. Reviews and updates the current:
 1. Security planning policy [Assignment: organization-defined frequency]; and
 2. Security planning procedures [Assignment: organization-defined frequency].

Supplemental Guidance

This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the PL family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

PL-2 SYSTEM SECURITY PLAN

PCF Compliance

Compliance with the requirements defined in this control is a deployer responsibility.

Pivotal provides [reference architecture](#) documents for each supported IaaS. This documentation may be helpful to an organization that needs to develop a system security plan. Specifically, the reference architecture documents describe the network topology and perimeter of a PCF deployment.

Control Description

The organization:

- a. 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 systems;
 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;
- b. Distributes copies of the security plan and communicates subsequent changes to the plan to [Assignment: organization-defined personnel or roles];
- c. Reviews the security plan for the information system [Assignment: organization-defined frequency];
- d. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and
- e. Protects the security plan from unauthorized disclosure and modification.

Supplemental Guidance

Security plans relate security requirements to a set of security controls and control enhancements. Security plans also describe, at a high level, how the security controls and control enhancements meet those security requirements, but do not provide detailed, technical descriptions of the specific design or implementation of the controls/enhancements. Security plans contain sufficient information (including the specification of parameter values for assignment and selection statements either explicitly or by reference) to enable a design and implementation that is unambiguously compliant with the intent of the plans and subsequent determinations of risk to organizational operations and assets, individuals, other organizations, and the Nation if the plan is implemented as intended. Organizations can also apply tailoring guidance to the security control baselines in Appendix D and CNSS Instruction 1253 to develop overlays for community-wide use or to address specialized requirements, technologies, or missions/environments of operation (e.g., DoD-tactical, Federal Public Key Infrastructure, or Federal Identity, Credential, and Access Management, space operations). Appendix I provides guidance on developing overlays. Security plans need not be single documents; the plans can be a collection of various documents including documents that already exist. Effective security plans make extensive use of references to policies, procedures, and additional documents (e.g., design and implementation specifications) where more detailed information can be obtained. This reduces the documentation requirements associated with security programs and maintains security-related information in other established management/operational areas related to enterprise architecture, system development life cycle, systems engineering, and acquisition. For example, security plans do not contain detailed contingency plan or incident response plan information but instead provide explicitly or by reference, sufficient information to define what needs to be accomplished by those plans.

PL-3 SYSTEM SECURITY PLAN UPDATE

PCF Compliance

Compliance with the requirements defined in this control is a deployer responsibility.

Control Description

[Withdrawn: Incorporated into PL-2].

Supplemental Guidance

PL-4 RULES OF BEHAVIOR

PCF Compliance

Compliance with the requirements defined in this control is a deployer responsibility.

Control Description

The organization:

- a. 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;
- b. 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;
- c. Reviews and updates the rules of behavior [Assignment: organization-defined frequency]; and
- d. Requires individuals who have signed a previous version of the rules of behavior to read and re-sign when the rules of behavior are revised/updated.

Supplemental Guidance

This control enhancement applies to organizational users. Organizations consider rules of behavior based on individual user roles and responsibilities, differentiating, for example, between rules that apply to privileged users and rules that apply to general users. Establishing rules of behavior for some types of non-organizational users including, for example, individuals who simply receive data/information from federal information systems, is often not feasible given the large number of such users and the limited nature of their interactions with the systems. Rules of behavior for both organizational and non-organizational users can also be established in AC-8, System Use Notification. PL-4 b. (the signed acknowledgment portion of this control) may be satisfied by the security awareness training and role-based security training programs conducted by organizations if such training includes rules of behavior. Organizations can use electronic signatures for acknowledging rules of behavior.

PL-5 PRIVACY IMPACT ASSESSMENT

PCF Compliance

Compliance with the requirements defined in this control is a deployer responsibility.

Control Description

[Withdrawn: Incorporated into Appendix J, AR-2].

Supplemental Guidance

PL-6 SECURITY-RELATED ACTIVITY PLANNING

PCF Compliance

Compliance with the requirements defined in this control is a deployer responsibility.

Control Description

[Withdrawn: Incorporated into PL-2].

Supplemental Guidance

PL-7 SECURITY CONCEPT OF OPERATIONS

PCF Compliance

Compliance with the requirements defined in this control are a deployer responsibility.

Organizations may reference the available Pivotal [PAS product documentation](#) when developing their security concept of operations.

Control Description

The organization:

- a. Develops a security Concept of Operations (CONOPS) for the information system containing at a minimum, how the organization intends to operate the system from the perspective of information security; and
- b. Reviews and updates the CONOPS [Assignment: organization-defined frequency].

Supplemental Guidance

The security CONOPS may be included in the security plan for the information system or in other system development life cycle-related documents, as appropriate. Changes to the CONOPS are reflected in ongoing updates to the security plan, the information security architecture, and other appropriate organizational documents (e.g., security specifications for procurements/acquisitions, system development life cycle documents, and systems/security engineering documents).

PL-8 INFORMATION SECURITY ARCHITECTURE

PCF Compliance

Compliance with the requirements defined in this control is a deployer responsibility.

Deployers should refer to the product documentation provided by Pivotal, including the [PAS reference architecture](#) for the appropriate IaaS, as well as the [operations](#) and [administration](#) guides.

The full set of product documentation is available on the [Pivotal Documentation](#) pages.

Control Description

The organization:

- a. 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;
- b. Reviews and updates the information security architecture [Assignment: organization-defined frequency] to reflect updates in the enterprise architecture; and
- c. Ensures that planned information security architecture changes are reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurements/acquisitions.

Supplemental Guidance

This control addresses actions taken by organizations in the design and development of information systems. The information security architecture at the individual information system level is consistent with and complements the more global, organization-wide information security architecture described in PM-7 that is integral to and developed as part of the enterprise architecture. The information security architecture includes an architectural description, the placement/allocation of security functionality (including security controls), security-related information for external interfaces, information being exchanged across the interfaces, and the protection mechanisms associated with each interface. In addition, the security architecture can include other important security-related information, for example, user roles and access privileges assigned to each role, unique security requirements, the types of information processed, stored, and transmitted by the information system, restoration priorities of information and information system services, and any other specific protection needs. In today's modern architecture, it is becoming less common for organizations to control all information resources. There are going to be key dependencies on external information services and service providers. Describing such dependencies in the information security architecture is important to developing a comprehensive mission/business protection strategy. Establishing, developing, documenting, and maintaining under configuration control, a baseline configuration for organizational information systems is critical to implementing and maintaining an effective information security architecture. The development of the information security architecture is coordinated with the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) to ensure that security controls needed to support privacy requirements are identified and effectively implemented. PL-8 is primarily directed at organizations (i.e., internally focused) to help ensure that organizations develop an information security architecture for the information system, and that the security architecture is integrated with or tightly coupled to the enterprise architecture through the organization-wide information security architecture. In contrast, SA-17 is primarily directed at external information technology product/system developers and integrators (although SA-17 could be used internally within organizations for in-house system development). SA-17, which is complementary to PL-8, is selected when organizations outsource the development of information systems or information system components to external entities, and there is a need to demonstrate/show consistency with the organization's enterprise architecture and information security architecture.

PL-9 CENTRAL MANAGEMENT

PCF Compliance

Compliance with the requirements defined in this control is a deployer responsibility.

Control Description

The organization centrally manages [Assignment: organization-defined security controls and related processes].

Supplemental Guidance

Central management refers to the organization-wide management and implementation of selected security controls and related processes. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed security controls and processes. As central management of security controls is generally associated with common controls, such management promotes and facilitates standardization of security control implementations and management and judicious use of organizational resources. Centrally-managed security controls and processes may also meet independence requirements for assessments in support of initial and ongoing authorizations to operate as part of organizational continuous monitoring. As part of the security control selection process, organizations determine which controls may be suitable for central management based on organizational resources and capabilities. Organizations consider that it may not always be possible to centrally manage every aspect of a security control. In such cases, the security control is treated as a hybrid control with the control managed and implemented either centrally or at the information system level. Controls and control enhancements that are candidates for full or partial central management include, but are not limited to: AC-2 (1) (2) (3) (4); AC-17 (1) (2) (3) (9); AC-18 (1) (3) (4) (5); AC-19 (4); AC-22; AC-23; AT-2 (1) (2); AT-3 (1) (2) (3); AT-4; AU-6 (1) (3) (5) (6) (9); AU-7 (1) (2); AU-11, AU-13, AU-16, CA-2 (1) (2) (3); CA-3 (1) (2) (3); CA-7 (1); CA-9; CM-2 (1) (2); CM-3 (1) (4); CM-4; CM-6 (1); CM-7 (4) (5); CM-8 (all); CM-9 (1); CM-10; CM-11; CP-7 (all); CP-8 (all); SC-43; SI-2; SI-3; SI-7; and SI-8.

Program Management Control Family

Number	Control	Pivotal Application Service (PAS) Compliance
PM-1	INFORMATION SECURITY PROGRAM PLAN	Inherited
PM-2	SENIOR INFORMATION SECURITY OFFICER	Not required for FISMA Moderate
PM-3	INFORMATION SECURITY RESOURCES	Not required for FISMA Moderate
PM-4	PLAN OF ACTION AND MILESTONES PROCESS	Not required for FISMA Moderate
PM-5	INFORMATION SYSTEM INVENTORY	Not required for FISMA Moderate
PM-6	INFORMATION SECURITY MEASURES OF PERFORMANCE	Not required for FISMA Moderate
PM-7	ENTERPRISE ARCHITECTURE	Not required for FISMA Moderate
PM-8	CRITICAL INFRASTRUCTURE PLAN	Not required for FISMA Moderate
PM-9	RISK MANAGEMENT STRATEGY	Not required for FISMA Moderate
PM-10	SECURITY AUTHORIZATION PROCESS	Not required for FISMA Moderate
PM-11	MISSION/BUSINESS PROCESS DEFINITION	Not required for FISMA Moderate
PM-12	INSIDER THREAT PROGRAM	Not required for FISMA Moderate
PM-13	INFORMATION SECURITY WORKFORCE	Not required for FISMA Moderate
PM-14	TESTING, TRAINING, AND MONITORING	Not required for FISMA Moderate
PM-15	CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS	Not required for FISMA Moderate
PM-16	THREAT AWARENESS PROGRAM	Not required for FISMA Moderate

PM-1 INFORMATION SECURITY PROGRAM PLAN

PCF Compliance

All dash-1 requirements are the responsibility of the deployer. Pivotal may be able to provide guidance to customers who are creating or updating documentation, but this documentation is unique to the deployer's mission and business goals. All implied required satisfied. PCF features are sufficient to satisfy PM-1.

Control Description

The organization:

- a. Develops and disseminates an organization-wide information security program plan that:
 1. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;
 2. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance;
 3. Reflects coordination among organizational entities responsible for the different aspects of information security (i.e., technical, physical, personnel, cyber-physical); and
 4. Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation;
- b. Reviews the organization-wide information security program plan [Assignment: organization-defined frequency];
- c. Updates the plan to address organizational changes and problems identified during plan implementation or security control assessments; and
- d. Protects the information security program plan from unauthorized disclosure and modification.

Supplemental Guidance

Information security program plans can be represented in single documents or compilations of documents at the discretion of organizations. The plans document the program management controls and organization-defined common controls. Information security program plans provide sufficient information about the program management controls/common controls (including specification of parameters for any assignment and selection statements either explicitly or by reference) to enable implementations that are unambiguously compliant with the intent of the plans and a determination of the risk to be incurred if the plans are implemented as intended. The security plans for individual information systems and the organization-wide information security program plan together, provide complete coverage for all security controls employed within the organization. Common controls are documented in an appendix to the organization's information security program plan unless the controls are included in a separate security plan for an information system (e.g., security controls employed as part of an intrusion detection system providing organization-wide boundary protection inherited by one or more organizational information systems). The organization-wide information security program plan will indicate which separate security plans contain descriptions of common controls. Organizations have the flexibility to describe common controls in a single document or in multiple documents. In the case of multiple documents, the documents describing common controls are included as attachments to the information security program plan. If the information security program plan contains multiple documents, the organization specifies in each document the organizational official or officials responsible for the development, implementation, assessment, authorization, and monitoring of the respective common controls. For example, the organization may require that the Facilities Management Office develop, implement, assess, authorize, and continuously monitor common physical and environmental protection controls from the PE family when such controls are not associated with a particular information system but instead, support multiple information systems.

PM-2 SENIOR INFORMATION SECURITY OFFICER

PCF Compliance

Not required for [FISMA](#) [Moderate](#).

Control Description

The organization appoints a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.

Supplemental Guidance

The security officer described in this control is an organizational official. For a federal agency (as defined in applicable federal laws, Executive Orders, directives, policies, or regulations) this official is the Senior Agency Information Security Officer. Organizations may also refer to this official as the Senior Information Security Officer or Chief Information Security Officer.

PM-3 INFORMATION SECURITY RESOURCES

PCF Compliance

Not required for [FISMA](#) [↗](#) Moderate.

Control Description

The organization:

- a. Ensures that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement;
- b. Employs a business case/Exhibit 300/Exhibit 53 to record the resources required; and
- c. Ensures that information security resources are available for expenditure as planned.

Supplemental Guidance

Organizations consider establishing champions for information security efforts and as part of including the necessary resources, assign specialized expertise and resources as needed. Organizations may designate and empower an Investment Review Board (or similar group) to manage and provide oversight for the information security-related aspects of the capital planning and investment control process.

PM-4 PLAN OF ACTION AND MILESTONES PROCESS

PCF Compliance

Not required for [FISMA](#) [Moderate](#).

Control Description

The organization:

- a. Implements a process for ensuring that plans of action and milestones for the security program and associated organizational information systems:
 1. Are developed and maintained;
 2. Document the remedial information security actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; and
 3. Are reported in accordance with OMB FISMA reporting requirements.
- b. Reviews plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

Supplemental Guidance

The plan of action and milestones is a key document in the information security program and is subject to federal reporting requirements established by OMB. With the increasing emphasis on organization-wide risk management across all three tiers in the risk management hierarchy (i.e., organization, mission/business process, and information system), organizations view plans of action and milestones from an organizational perspective, prioritizing risk response actions and ensuring consistency with the goals and objectives of the organization. Plan of action and milestones updates are based on findings from security control assessments and continuous monitoring activities. OMB FISMA reporting guidance contains instructions regarding organizational plans of action and milestones.

PM-5 INFORMATION SYSTEM INVENTORY

PCF Compliance

Not required for [FISMA](#) Moderate.

Control Description

The organization develops and maintains an inventory of its information systems.

Supplemental Guidance

This control addresses the inventory requirements in FISMA. OMB provides guidance on developing information systems inventories and associated reporting requirements. For specific information system inventory reporting requirements, organizations consult OMB annual FISMA reporting guidance.

PM-6 INFORMATION SECURITY MEASURES OF PERFORMANCE

PCF Compliance

Not required for [FISMA](#) [↗](#) Moderate.

Control Description

The organization develops, monitors, and reports on the results of information security measures of performance.

Supplemental Guidance

Measures of performance are outcome-based metrics used by an organization to measure the effectiveness or efficiency of the information security program and the security controls employed in support of the program.

PM-7 ENTERPRISE ARCHITECTURE

PCF Compliance

Not required for [FISMA](#) [Moderate](#).

Control Description

The organization develops an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation.

Supplemental Guidance

The enterprise architecture developed by the organization is aligned with the Federal Enterprise Architecture. The integration of information security requirements and associated security controls into the organization's enterprise architecture helps to ensure that security considerations are addressed by organizations early in the system development life cycle and are directly and explicitly related to the organization's mission/business processes. This process of security requirements integration also embeds into the enterprise architecture, an integral information security architecture consistent with organizational risk management and information security strategies. For PM-7, the information security architecture is developed at a system-of-systems level (organization-wide), representing all of the organizational information systems. For PL-8, the information security architecture is developed at a level representing an individual information system but at the same time, is consistent with the information security architecture defined for the organization. Security requirements and security control integration are most effectively accomplished through the application of the Risk Management Framework and supporting security standards and guidelines. The Federal Segment Architecture Methodology provides guidance on integrating information security requirements and security controls into enterprise architectures.

PM-8 CRITICAL INFRASTRUCTURE PLAN

PCF Compliance

Not required for [FISMA](#) [↗](#) Moderate.

Control Description

The organization addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.

Supplemental Guidance

Protection strategies are based on the prioritization of critical assets and resources. The requirement and guidance for defining critical infrastructure and key resources and for preparing an associated critical infrastructure protection plan are found in applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

PM-9 RISK MANAGEMENT STRATEGY

PCF Compliance

Not required for [FISMA](#) [↗](#) Moderate.

Control Description

The organization:

- a. Develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems;
- b. Implements the risk management strategy consistently across the organization; and
- c. Reviews and updates the risk management strategy [Assignment: organization-defined frequency] or as required, to address organizational changes.

Supplemental Guidance

An organization-wide risk management strategy includes, for example, an unambiguous expression of the risk tolerance for the organization, acceptable risk assessment methodologies, risk mitigation strategies, a process for consistently evaluating risk across the organization with respect to the organization's risk tolerance, and approaches for monitoring risk over time. The use of a risk executive function can facilitate consistent, organization-wide application of the risk management strategy. The organization-wide risk management strategy can be informed by risk-related inputs from other sources both internal and external to the organization to ensure the strategy is both broad-based and comprehensive.

PM-10 SECURITY AUTHORIZATION PROCESS

PCF Compliance

Not required for [FISMA](#) [↗](#) Moderate.

Control Description

The organization:

- a. Manages (i.e., documents, tracks, and reports) the security state of organizational information systems and the environments in which those systems operate through security authorization processes;
- b. Designates individuals to fulfill specific roles and responsibilities within the organizational risk management process; and
- c. Fully integrates the security authorization processes into an organization-wide risk management program.

Supplemental Guidance

Security authorization processes for information systems and environments of operation require the implementation of an organization-wide risk management process, a Risk Management Framework, and associated security standards and guidelines. Specific roles within the risk management process include an organizational risk executive (function) and designated authorizing officials for each organizational information system and common control provider. Security authorization processes are integrated with organizational continuous monitoring processes to facilitate ongoing understanding and acceptance of risk to organizational operations and assets, individuals, other organizations, and the Nation.

PM-11 MISSION/BUSINESS PROCESS DEFINITION

PCF Compliance

Not required for [FISMA](#) [Moderate](#).

Control Description

The organization:

- a. Defines mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and
- b. Determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until achievable protection needs are obtained.

Supplemental Guidance

Information protection needs are technology-independent, required capabilities to counter threats to organizations, individuals, or the Nation through the compromise of information (i.e., loss of confidentiality, integrity, or availability). Information protection needs are derived from the mission/business needs defined by the organization, the mission/business processes selected to meet the stated needs, and the organizational risk management strategy. Information protection needs determine the required security controls for the organization and the associated information systems supporting the mission/business processes. Inherent in defining an organization's information protection needs is an understanding of the level of adverse impact that could result if a compromise of information occurs. The security categorization process is used to make such potential impact determinations. Mission/business process definitions and associated information protection requirements are documented by the organization in accordance with organizational policy and procedure.

PM-12 INSIDER THREAT PROGRAM

PCF Compliance

Not required for [FISMA](#) [Moderate](#).

Control Description

The organization implements an insider threat program that includes a cross-discipline insider threat incident handling team.

Supplemental Guidance

Organizations handling classified information are required, under Executive Order 13587 and the National Policy on Insider Threat, to establish insider threat programs. The standards and guidelines that apply to insider threat programs in classified environments can also be employed effectively to improve the security of Controlled Unclassified Information in non-national security systems. Insider threat programs include security controls to detect and prevent malicious insider activity through the centralized integration and analysis of both technical and non-technical information to identify potential insider threat concerns. A senior organizational official is designated by the department/agency head as the responsible individual to implement and provide oversight for the program. In addition to the centralized integration and analysis capability, insider threat programs as a minimum, prepare department/agency insider threat policies and implementation plans, conduct host-based user monitoring of individual employee activities on government-owned classified computers, provide insider threat awareness training to employees, receive access to information from all offices within the department/agency (e.g., human resources, legal, physical security, personnel security, information technology, information system security, and law enforcement) for insider threat analysis, and conduct self-assessments of department/agency insider threat posture. Insider threat programs can leverage the existence of incident handling teams organizations may already have in place, such as computer security incident response teams. Human resources records are especially important in this effort, as there is compelling evidence to show that some types of insider crimes are often preceded by nontechnical behaviors in the workplace (e.g., ongoing patterns of disgruntled behavior and conflicts with coworkers and other colleagues). These precursors can better inform and guide organizational officials in more focused, targeted monitoring efforts. The participation of a legal team is important to ensure that all monitoring activities are performed in accordance with appropriate legislation, directives, regulations, policies, standards, and guidelines.

PM-13 INFORMATION SECURITY WORKFORCE

PCF Compliance

Not required for [FISMA](#) [Moderate](#).

Control Description

The organization establishes an information security workforce development and improvement program.

Supplemental Guidance

Information security workforce development and improvement programs include, for example: (i) defining the knowledge and skill levels needed to perform information security duties and tasks; (ii) developing role-based training programs for individuals assigned information security roles and responsibilities; and (iii) providing standards for measuring and building individual qualifications for incumbents and applicants for information security-related positions. Such workforce programs can also include associated information security career paths to encourage: (i) information security professionals to advance in the field and fill positions with greater responsibility; and (ii) organizations to fill information security-related positions with qualified personnel. Information security workforce development and improvement programs are complementary to organizational security awareness and training programs. Information security workforce development and improvement programs focus on developing and institutionalizing core information security capabilities of selected personnel needed to protect organizational operations, assets, and individuals.

PM-14 TESTING, TRAINING, AND MONITORING

PCF Compliance

Not required for [FISMA](#) [Moderate](#).

Control Description

The organization:

- a. Implements a process for ensuring that organizational plans for conducting security testing, training, and monitoring activities associated with organizational information systems:
 - 1. Are developed and maintained; and
 - 2. Continue to be executed in a timely manner;
- b. Reviews testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

Supplemental Guidance

This control ensures that organizations provide oversight for the security testing, training, and monitoring activities conducted organization-wide and that those activities are coordinated. With the importance of continuous monitoring programs, the implementation of information security across the three tiers of the risk management hierarchy, and the widespread use of common controls, organizations coordinate and consolidate the testing and monitoring activities that are routinely conducted as part of ongoing organizational assessments supporting a variety of security controls. Security training activities, while typically focused on individual information systems and specific roles, also necessitate coordination across all organizational elements. Testing, training, and monitoring plans and activities are informed by current threat and vulnerability assessments.

PM-15 CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS

PCF Compliance

Not required for [FISMA](#) [Moderate](#).

Control Description

The organization establishes and institutionalizes contact with selected groups and associations within the security community:

- a. To facilitate ongoing security education and training for organizational personnel;
- b. To maintain currency with recommended security practices, techniques, and technologies; and
- c. To share current security-related information including threats, vulnerabilities, and incidents.

Supplemental Guidance

Ongoing contact with security groups and associations is of paramount importance in an environment of rapidly changing technologies and threats. Security groups and associations include, for example, special interest groups, forums, professional associations, news groups, and/or peer groups of security professionals in similar organizations. Organizations select groups and associations based on organizational missions/business functions. Organizations share threat, vulnerability, and incident information consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

PM-16 THREAT AWARENESS PROGRAM

PCF Compliance

Not required for [FISMA](#) [Moderate](#).

Control Description

The organization implements a threat awareness program that includes a cross-organization information-sharing capability.

Supplemental Guidance

Because of the constantly changing and increasing sophistication of adversaries, especially the advanced persistent threat (APT), it is becoming more likely that adversaries may successfully breach or compromise organizational information systems. One of the best techniques to address this concern is for organizations to share threat information. This can include, for example, sharing threat events (i.e., tactics, techniques, and procedures) that organizations have experienced, mitigations that organizations have found are effective against certain types of threats, threat intelligence (i.e., indications and warnings about threats that are likely to occur). Threat information sharing may be bilateral (e.g., government-commercial cooperatives, government-government cooperatives), or multilateral (e.g., organizations taking part in threat-sharing consortia). Threat information may be highly sensitive requiring special agreements and protection, or less sensitive and freely shared.

Risk Assessment Control Family

Number	Control	Pivotal Application Service (PAS) Compliance
RA-1	RISK ASSESSMENT POLICY AND PROCEDURES	Deployer responsibility
RA-2	SECURITY CATEGORIZATION	Deployer responsibility
RA-3	RISK ASSESSMENT	Deployer responsibility
RA-4	RISK ASSESSMENT UPDATE	Deployer responsibility
RA-5	VULNERABILITY SCANNING	Compliant
RA-6	TECHNICAL SURVEILLANCE COUNTERMEASURES SURVEY	P0, so not required for FISMA Moderate

RA-1 RISK ASSESSMENT POLICY AND PROCEDURES

PCF Compliance

All xx-1 requirements are the responsibility of the deployer. The PCF product feature set is sufficient to satisfy the technical requirements implied in RA-1. Pivotal may be able to provide guidance to customers who are creating or updating documentation, but this documentation is unique to the deployer's mission and business goals.

Control Description

The organization:

- a. 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
- b. Reviews and updates the current:
 1. Risk assessment policy [Assignment: organization-defined frequency]; and
 2. Risk assessment procedures [Assignment: organization-defined frequency].

Supplemental Guidance

This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the RA family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

RA-2 SECURITY CATEGORIZATION

PCF Compliance

Compliance with the requirements defined in this control is a deployer responsibility.

Control Description

The organization:

- a. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
- b. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and
- c. Ensures that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision

Supplemental Guidance

Clearly defined authorization boundaries are a prerequisite for effective security categorization decisions. Security categories describe the potential adverse impacts to organizational operations, organizational assets, and individuals if organizational information and information systems are comprised through a loss of confidentiality, integrity, or availability. Organizations conduct the security categorization process as an organization-wide activity with the involvement of chief information officers, senior information security officers, information system owners, mission/business owners, and information owners/stewards. Organizations also consider the potential adverse impacts to other organizations and, in accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives, potential national-level adverse impacts. Security categorization processes carried out by organizations facilitate the development of inventories of information assets, and along with CM-8, mappings to specific information system components where information is processed, stored, or transmitted.

RA-3 RISK ASSESSMENT

PCF Compliance

Compliance with the requirements defined in this control is a deployer responsibility.

Control Description

The organization:

- a. 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;
- b. Documents risk assessment results in [Selection: security plan; risk assessment report; [Assignment: organization-defined document]];
- c. Reviews risk assessment results [Assignment: organization-defined frequency];
- d. Disseminates risk assessment results to [Assignment: organization-defined personnel or roles]; and
- e. Updates the risk assessment [Assignment: organization-defined frequency] 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.

Supplemental Guidance

Clearly defined authorization boundaries are a prerequisite for effective risk assessments. Risk assessments take into account threats, vulnerabilities, likelihood, and impact to organizational operations and assets, individuals, other organizations, and the Nation based on the operation and use of information systems. Risk assessments also take into account risk from external parties (e.g., service providers, contractors operating information systems on behalf of the organization, individuals accessing organizational information systems, outsourcing entities). In accordance with OMB policy and related E-authentication initiatives, authentication of public users accessing federal information systems may also be required to protect nonpublic or privacy-related information. As such, organizational assessments of risk also address public access to federal information systems. Risk assessments (either formal or informal) can be conducted at all three tiers in the risk management hierarchy (i.e., organization level, mission/business process level, or information system level) and at any phase in the system development life cycle. Risk assessments can also be conducted at various steps in the Risk Management Framework, including categorization, security control selection, security control implementation, security control assessment, information system authorization, and security control monitoring. RA-3 is noteworthy in that the control must be partially implemented prior to the implementation of other controls in order to complete the first two steps in the Risk Management Framework. Risk assessments can play an important role in security control selection processes, particularly during the application of tailoring guidance, which includes security control supplementation.

RA-4 RISK ASSESSMENT UPDATE

PCF Compliance

Compliance with the requirements defined in this control is a deployer responsibility.

Control Description

[Withdrawn: Incorporated into RA-3].

Supplemental Guidance

RA-5 VULNERABILITY SCANNING

PCF Compliance

In general, PCF satisfies all technical requirements implied by this control. PCF supports the use of third-party scanners, either using remote access scanning, or using local installation of third-party agents on the BOSH stemcells. Pivotal has defined an appropriate configuration benchmark to assist organizations assessing the security posture of a PCF deployment. The deployer is responsible for performing scans for both configuration and vulnerabilities. Customers performing configuration scans against a PCF deployment should adjust their scanning benchmark to perform a cloud-native assessment, as opposed to employing a scanning benchmark intended for standalone Linux server deployments. Customers requiring assistance with scanning a deployment may contact Pivotal Security Team at security@pivotal.io.

Control Description

The organization:

- a. Scans for vulnerabilities in the information system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system/applications are identified and reported;
- b. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
 1. Enumerating platforms, software flaws, and improper configurations;
 2. Formatting checklists and test procedures; and
 3. Measuring vulnerability impact;
- c. Analyzes vulnerability scan reports and results from security control assessments;
- d. Remediates legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk; and
- e. 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).

Supplemental Guidance

Security categorization of information systems guides the frequency and comprehensiveness of vulnerability scans. Organizations determine the required vulnerability scanning for all information system components, ensuring that potential sources of vulnerabilities such as networked printers, scanners, and copiers are not overlooked. Vulnerability analyses for custom software applications may require additional approaches such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Organizations can employ these analysis approaches in a variety of tools (e.g., web-based application scanners, static analysis tools, binary analyzers) and in source code reviews. Vulnerability scanning includes, for example: (i) scanning for patch levels; (ii) scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and (iii) scanning for improperly configured or incorrectly operating information flow control mechanisms. Organizations consider using tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and that use the Open Vulnerability Assessment Language (OVAL) to determine/test for the presence of vulnerabilities. Suggested sources for vulnerability information include the Common Weakness Enumeration (CWE) listing and the National Vulnerability Database (NVD). In addition, security control assessments such as red team exercises provide other sources of potential vulnerabilities for which to scan. Organizations also consider using tools that express vulnerability impact by the Common Vulnerability Scoring System (CVSS).

RA-6 TECHNICAL SURVEILLANCE COUNTERMEASURES SURVEY

PCF Compliance

P0, so not required for FISMA Moderate.

Control Description

The organization employs a technical surveillance countermeasures survey at [Assignment: organization-defined locations] [Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined events or indicators occur]].

Supplemental Guidance

Technical surveillance countermeasures surveys are performed by qualified personnel to detect the presence of technical surveillance devices/hazards and to identify technical security weaknesses that could aid in the conduct of technical penetrations of surveyed facilities. Such surveys provide evaluations of the technical security postures of organizations and facilities and typically include thorough visual, electronic, and physical examinations in and about surveyed facilities. The surveys also provide useful input into risk assessments and organizational exposure to potential adversaries.

CA - Security Assessment and Authorization Control Family

Number	Control	Pivotal Application Service (PAS) Compliance
CA-1	SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES	Inherited and Compliant
CA-2	SECURITY ASSESSMENTS	Inherited
CA-3	SYSTEM INTERCONNECTIONS	Inherited and Compliant
CA-5	PLAN OF ACTION AND MILESTONES	Inherited
CA-6	SECURITY AUTHORIZATION	Inherited
CA-7	CONTINUOUS MONITORING	Inherited and Compliant
CA-8	PENETRATION TESTING	Not required for FISMA Moderate
CA-9	INTERNAL SYSTEM CONNECTIONS	Inherited

CA-1 SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES

PCF Compliance

All dash-1 requirements are the responsibility of the deployer. Pivotal may be able to provide guidance to customers who are creating or updating documentation, but this documentation is unique to the deployer's mission / business goals. All implied required satisfied. PCF features are sufficient to satisfy CA-1.

Control Description

The organization:

- a. 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
- b. Reviews and updates the current:
 - 1. Security assessment and authorization policy [Assignment: organization-defined frequency]; and
 - 2. Security assessment and authorization procedures [Assignment: organization-defined frequency].

Supplemental Guidance

This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the CA family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

CA-2 SECURITY ASSESSMENTS

PCF Compliance

Deployers can use this NIST Controls for PCF documentation and [PCF documentation](#) to help develop a security assessment plan.

Deployers may use automated scanning tools to assess the security of their specific deployments. Pivotal performs regular port, configuration, and vulnerability scans on its own PCF deployments.

The [PCF Security Guide](#) explains the ongoing procedures that Pivotal follows to assess and maintain the security of PCF.

Control Description

The organization:

- a. 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;
- b. Assesses the security controls in the information system and its environment of operation [Assignment: organization-defined frequency] 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;
- c. Produces a security assessment report that documents the results of the assessment; and
- d. Provides the results of the security control assessment to [Assignment: organization-defined individuals or roles].

Supplemental Guidance

Organizations assess security controls in organizational information systems and the environments in which those systems operate as part of: (i) initial and ongoing security authorizations; (ii) FISMA annual assessments; (iii) continuous monitoring; and (iv) system development life cycle activities. Security assessments: (i) ensure that information security is built into organizational information systems; (ii) identify weaknesses and deficiencies early in the development process; (iii) provide essential information needed to make risk-based decisions as part of security authorization processes; and (iv) ensure compliance to vulnerability mitigation procedures. Assessments are conducted on the implemented security controls from Appendix F (main catalog) and Appendix G (Program Management controls) as documented in System Security Plans and Information Security Program Plans. Organizations can use other types of assessment activities such as vulnerability scanning and system monitoring to maintain the security posture of information systems during the entire life cycle. Security assessment reports document assessment results in sufficient detail as deemed necessary by organizations, to determine the accuracy and completeness of the reports and whether the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting security requirements. The FISMA requirement for assessing security controls at least annually does not require additional assessment activities to those activities already in place in organizational security authorization processes. Security assessment results are provided to the individuals or roles appropriate for the types of assessments being conducted. For example, assessments conducted in support of security authorization decisions are provided to authorizing officials or authorizing official designated representatives. To satisfy annual assessment requirements, organizations can use assessment results from the following sources: (i) initial or ongoing information system authorizations; (ii) continuous monitoring; or (iii) system development life cycle activities. Organizations ensure that security assessment results are current, relevant to the determination of security control effectiveness, and obtained with the appropriate level of assessor independence. Existing security control assessment results can be reused to the extent that the results are still valid and can also be supplemented with additional assessments as needed. Subsequent to initial authorizations and in accordance with OMB policy, organizations assess security controls during continuous monitoring. Organizations establish the frequency for ongoing security control assessments in accordance with organizational continuous monitoring strategies. Information Assurance Vulnerability Alerts provide useful examples of vulnerability mitigation procedures. External audits (e.g., audits by external entities such as regulatory agencies) are outside the scope of this control.

CA-3 SYSTEM INTERCONNECTIONS

PCF Compliance

Compliance with this requirement is the responsibility of the PCF deployer.

Outgoing traffic from PCF applications is controlled by [Application Security Groups](#).

Applications running on PCF can communicate with user-provided and brokered services running outside of PCF. The deployer controls access to these outboard services through RBAC enforcements in the Cloud Controller.

Control Description

The organization:

- a. Authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements;
- b. Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and
- c. Reviews and updates Interconnection Security Agreements [Assignment: organization-defined frequency].

Supplemental Guidance

This control applies to dedicated connections between information systems (i.e., system interconnections) and does not apply to transitory, user-controlled connections such as email and website browsing. Organizations carefully consider the risks that may be introduced when information systems are connected to other systems with different security requirements and security controls, both within organizations and external to organizations. Authorizing officials determine the risk associated with information system connections and the appropriate controls employed. If interconnecting systems have the same authorizing official, organizations do not need to develop Interconnection Security Agreements. Instead, organizations can describe the interface characteristics between those interconnecting systems in their respective security plans. If interconnecting systems have different authorizing officials within the same organization, organizations can either develop Interconnection Security Agreements or describe the interface characteristics between systems in the security plans for the respective systems. Organizations may also incorporate Interconnection Security Agreement information into formal contracts, especially for interconnections established between federal agencies and nonfederal (i.e., private sector) organizations. Risk considerations also include information systems sharing the same networks. For certain technologies (e.g., space, unmanned aerial vehicles, and medical devices), there may be specialized connections in place during pre-operational testing. Such connections may require Interconnection Security Agreements and be subject to additional security controls.

CA-5 PLAN OF ACTION AND MILESTONES

PCF Compliance

Compliance with this requirement is the responsibility of the PCF deployer.

Control Description

The organization:

- a. 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
- b. Updates existing plan of action and milestones [Assignment: organization-defined frequency] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

Supplemental Guidance

Plans of action and milestones are key documents in security authorization packages and are subject to federal reporting requirements established by OMB.

CA-6 SECURITY AUTHORIZATION

PCF Compliance

Compliance with this requirement is the responsibility of the PCF deployer.

Control Description

The organization:

- a. Assigns a senior-level executive or manager as the authorizing official for the information system;
- b. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and
- c. Updates the security authorization [Assignment: organization-defined frequency].

Supplemental Guidance

Security authorizations are official management decisions, conveyed through authorization decision documents, by senior organizational officials or executives (i.e., authorizing officials) to authorize operation of information systems and to explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the Nation based on the implementation of agreed-upon security controls. Authorizing officials provide budgetary oversight for organizational information systems or assume responsibility for the mission/business operations supported by those systems. The security authorization process is an inherently federal responsibility and therefore, authorizing officials must be federal employees. Through the security authorization process, authorizing officials assume responsibility and are accountable for security risks associated with the operation and use of organizational information systems. Accordingly, authorizing officials are in positions with levels of authority commensurate with understanding and accepting such information security-related risks. OMB policy requires that organizations conduct ongoing authorizations of information systems by implementing continuous monitoring programs. Continuous monitoring programs can satisfy three-year reauthorization requirements, so separate reauthorization processes are not necessary. Through the employment of comprehensive continuous monitoring processes, critical information contained in authorization packages (i.e., security plans, security assessment reports, and plans of action and milestones) is updated on an ongoing basis, providing authorizing officials and information system owners with an up-to-date status of the security state of organizational information systems and environments of operation. To reduce the administrative cost of security reauthorization, authorizing officials use the results of continuous monitoring processes to the maximum extent possible as the basis for rendering reauthorization decisions.

CA-7 CONTINUOUS MONITORING

PCF Compliance

Compliance with this requirement is the responsibility of the PCF deployer.

PCF supports third-party security scanning, either through remote access, or through local installation of a third-party agent on the stemcell as a BOSH add-on.

Pivotal has defined an SCAP v1.3-compliant benchmark for BOSH stemcells.

Control Description

The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes:

- a. Establishment of [Assignment: organization-defined metrics] to be monitored;
- b. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring;
- c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy;
- d. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy;
- e. Correlation and analysis of security-related information generated by assessments and monitoring;
- f. Response actions to address results of the analysis of security-related information; and
- g. Reporting the security status of organization and the information system to [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency].

Supplemental Guidance

Continuous monitoring programs facilitate ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions. The terms continuous and ongoing imply that organizations assess/analyze security controls and information security-related risks at a frequency sufficient to support organizational risk-based decisions. The results of continuous monitoring programs generate appropriate risk response actions by organizations. Continuous monitoring programs also allow organizations to maintain the security authorizations of information systems and common controls over time in highly dynamic environments of operation with changing mission/business needs, threats, vulnerabilities, and technologies. Having access to security-related information on a continuing basis through reports/dashboards gives organizational officials the capability to make more effective and timely risk management decisions, including ongoing security authorization decisions. Automation supports more frequent updates to security authorization packages, hardware/software/firmware inventories, and other system information. Effectiveness is further enhanced when continuous monitoring outputs are formatted to provide information that is specific, measurable, actionable, relevant, and timely. Continuous monitoring activities are scaled in accordance with the security categories of information systems.

CA-8 PENETRATION TESTING

PCF Compliance

This control is not required for FISMA moderate.

Control Description

The organization conducts penetration testing [Assignment: organization-defined frequency] on [Assignment: organization-defined information systems or system components].

Supplemental Guidance

Penetration testing is a specialized type of assessment conducted on information systems or individual system components to identify vulnerabilities that could be exploited by adversaries. Such testing can be used to either validate vulnerabilities or determine the degree of resistance organizational information systems have to adversaries within a set of specified constraints (e.g., time, resources, and/or skills). Penetration testing attempts to duplicate the actions of adversaries in carrying out hostile cyber attacks against organizations and provides a more in-depth analysis of security-related weaknesses/deficiencies. Organizations can also use the results of vulnerability analyses to support penetration testing activities. Penetration testing can be conducted on the hardware, software, or firmware components of an information system and can exercise both physical and technical security controls. A standard method for penetration testing includes, for example: (i) pretest analysis based on full knowledge of the target system; (ii) pretest identification of potential vulnerabilities based on pretest analysis; and (iii) testing designed to determine exploitability of identified vulnerabilities. All parties agree to the rules of engagement before the commencement of penetration testing scenarios. Organizations correlate the penetration testing rules of engagement with the tools, techniques, and procedures that are anticipated to be employed by adversaries carrying out attacks. Organizational risk assessments guide decisions on the level of independence required for personnel conducting penetration testing.

CA-9 INTERNAL SYSTEM CONNECTIONS

PCF Compliance

Compliance with this requirement is the responsibility of the PCF deployer.

Control Description

The organization:

- a. Authorizes internal connections of [Assignment: organization-defined information system components or classes of components] to the information system; and
- b. Documents, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated.

Supplemental Guidance

This control applies to connections between organizational information systems and (separate) constituent system components (i.e., intra-system connections) including, for example, system connections with mobile devices, notebook/desktop computers, printers, copiers, facsimile machines, scanners, sensors, and servers. Instead of authorizing each individual internal connection, organizations can authorize internal connections for a class of components with common characteristics and/or configurations, for example, all digital printers, scanners, and copiers with a specified processing, storage, and transmission capability or all smart phones with a specific baseline configuration.

System And Communications Protection Control Family

Number	Control	Pivotal Application Service (PAS) Compliance
SC-1	SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES	Deployer responsibility
SC-2	APPLICATION PARTITIONING	Compliant
SC-3	SECURITY FUNCTION ISOLATION	Not applicable
SC-4	INFORMATION IN SHARED RESOURCES	Compliant
SC-5	DENIAL OF SERVICE PROTECTION	Compliant and inherited
SC-6	RESOURCE AVAILABILITY	P0, so not required for FISMA Moderate
SC-7	BOUNDARY PROTECTION	Compliant and inherited
SC-8	TRANSMISSION CONFIDENTIALITY AND INTEGRITY	Compliant
SC-9	TRANSMISSION CONFIDENTIALITY	Not applicable
SC-10	NETWORK DISCONNECT	Compliant and inherited
SC-11	TRUSTED PATH	Not applicable
SC-12	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	Compliant and inherited
SC-13	CRYPTOGRAPHIC PROTECTION	Inherited and compliant
SC-14	PUBLIC ACCESS PROTECTIONS	Not applicable
SC-15	COLLABORATIVE COMPUTING DEVICES	Deployer responsibility
SC-16	TRANSMISSION OF SECURITY ATTRIBUTES	P0, so not required for FISMA Moderate
SC-17	PUBLIC KEY INFRASTRUCTURE CERTIFICATES	Compliant
SC-18	MOBILE CODE	Compliant
SC-19	VOICE OVER INTERNET PROTOCOL	Deployer responsibility
SC-20	SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)	Compliant and inherited
SC-21	SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)	Compliant and inherited
SC-22	ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE	Compliant and inherited
SC-23	SESSION AUTHENTICITY	Compliant
SC-24	FAIL IN KNOWN STATE	P1, not required for FISMA Moderate
SC-25	THIN NODES	P0, not required for FISMA Moderate
SC-26	HONEYPOTS	P0, not required for FISMA Moderate
SC-27	PLATFORM-INDEPENDENT APPLICATIONS	P0, not required for FISMA Moderate
SC-28	PROTECTION OF INFORMATION AT REST	Compliant and inherited
SC-29	HETEROGENEITY	P0, not required for FISMA Moderate
SC-30	CONCEALMENT AND MISDIRECTION	P0, not required for FISMA Moderate
SC-31	COVERT CHANNEL ANALYSIS	P0, not required for FISMA Moderate
SC-32	INFORMATION SYSTEM PARTITIONING	P0, not required for FISMA Moderate
SC-33	TRANSMISSION PREPARATION INTEGRITY	Not applicable
SC-34	NON-MODIFIABLE EXECUTABLE PROGRAMS	P0, not required for FISMA Moderate
SC-35	HONEYCLIENTS	P0, not required for FISMA Moderate
SC-36	DISTRIBUTED PROCESSING AND STORAGE	P0, not required for FISMA Moderate
SC-37	OUT-OF-BAND CHANNELS	P0, not required for FISMA Moderate
SC-38	OPERATIONS SECURITY	P0, not required for FISMA Moderate
SC-39	PROCESS ISOLATION	Compliant
SC-40	WIRELESS LINK PROTECTION	P0, not required for FISMA Moderate
SC-41	PORT AND I/O DEVICE ACCESS	P0, not required for FISMA Moderate
SC-42	SENSOR CAPABILITY AND DATA	P0, not required for FISMA Moderate
SC-43	USAGE RESTRICTIONS	P0, not required for FISMA Moderate
SC-44	DETONATION CHAMBERS	P0, not required for FISMA Moderate

SC-1 SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES

PCF Compliance

All xx-1 requirements are the responsibility of the deployer. The PCF product feature set is sufficient to satisfy the technical requirements implied in SC-1. Pivotal may be able to provide guidance to customers who are creating or updating documentation, but this documentation is unique to the deployer's mission and business goals.

Control Description

The organization:

- a. 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
- b. Reviews and updates the current:
 1. System and communications protection policy [Assignment: organization-defined frequency]; and
 2. System and communications protection procedures [Assignment: organization-defined frequency].

Supplemental Guidance

This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the SC family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

SC-2 APPLICATION PARTITIONING

PCF Compliance

A PCF PAS deployment is managed via the BOSH CLI and/or the Ops Manager UI. When deployed in compliance with Pivotal reference architecture, the PCF PAS is compliant with the requirements in this control.

Regular users accessing the applications on the platform cannot access the BOSH director or the Ops Manager interface, which are expected to be running on a separate (non-routable) network / vLAN.

In addition, the DevOps users of the platform may be given different RBAC roles in the Cloud Controller, to appropriately limit their authorization level, depending upon if they are a developer, auditor, manager, and so on.

Access control for applications is the responsibility of the application developer.

More information is available about the PCF PAS [reference architecture](#) for each supported IaaS platform. More information is available about the [RBAC controls](#) present in the Cloud Foundry Cloud Controller. Additional information is also available on Cloud Foundry [security concepts](#).

Control Description

The information system separates user functionality (including user interface services) from information system management functionality.

Supplemental Guidance

Information system management functionality includes, for example, functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access. The separation of user functionality from information system management functionality is either physical or logical. Organizations implement separation of system management-related functionality from user functionality by using different computers, different central processing units, different instances of operating systems, different network addresses, virtualization techniques, or combinations of these or other methods, as appropriate. This type of separation includes, for example, web administrative interfaces that use separate authentication methods for users of any other information system resources. Separation of system and user functionality may include isolating administrative interfaces on different domains and with additional access controls.

SC-3 SECURITY FUNCTION ISOLATION

PCF Compliance

Not Applicable.

This requirement is not in scope for systems operating at the FISMA Moderate level.

However, PCF PAS is compliant with the intent of these requirements.

PCF PAS implements best practice recommendations to ensure that applications hosted on the platform are isolated from privileged security functions. The PAS Diego container runtime uses isolation constructs such as user namespaces, overlay filesystems, container network configurations, CPU cgroups, Ubuntu AppArmor profiles, and seccomp kernel restrictions to ensure that unprivileged applications may not adversely impact the platform's core security functions.

Control Description

The information system isolates security functions from nonsecurity functions.

Supplemental Guidance

The information system isolates security functions from nonsecurity functions by means of an isolation boundary (implemented via partitions and domains). Such isolation controls access to and protects the integrity of the hardware, software, and firmware that perform those security functions. Information systems implement code separation (i.e., separation of security functions from nonsecurity functions) in a number of ways, including, for example, through the provision of security kernels via processor rings or processor modes. For non-kernel code, security function isolation is often achieved through file system protections that serve to protect the code on disk, and address space protections that protect executing code. Information systems restrict access to security functions through the use of access control mechanisms and by implementing least privilege capabilities. While the ideal is for all of the code within the security function isolation boundary to only contain security-relevant code, it is sometimes necessary to include nonsecurity functions within the isolation boundary as an exception.

SC-4 INFORMATION IN SHARED RESOURCES

PCF Compliance

PCF PAS runs applications inside [linux containers](#) [↗](#).

These linux containers are designed to provide isolation between application processes, including filesystem, network, memory, and CPU.

In particular, the container filesystem is created using an overlay FS, ensuring that disk writes from one application cannot be seen by another concurrent or future application executing on the same host.

In addition, the containers are run on BOSH managed VMs which are themselves relatively short-lived. These VMs are created with both ephemeral and persistent disks, and all transient application data is stored on ephemeral disks, which are not preserved when a VM is recreated.

More information on how BOSH manages disk storage may be found in the [BOSH documentation](#) [↗](#).

Control Description

The information system prevents unauthorized and unintended information transfer via shared system resources.

Supplemental Guidance

This control prevents information, including encrypted representations of information, produced by the actions of prior users/roles (or the actions of processes acting on behalf of prior users/roles) from being available to any current users/roles (or current processes) that obtain access to shared system resources (e.g., registers, main memory, hard disks) after those resources have been released back to information systems. The control of information in shared resources is also commonly referred to as object reuse and residual information protection. This control does not address: (i) information remanence which refers to residual representation of data that has been nominally erased or removed; (ii) covert channels (including storage and/or timing channels) where shared resources are manipulated to violate information flow restrictions; or (iii) components within information systems for which there are only single users/roles.

SC-5 DENIAL OF SERVICE PROTECTION

PCF Compliance

As described in the corresponding [reference architecture](#) documentation, the PCF PAS deployment depends upon the presence of an IaaS firewall and load balancer infrastructure. The PCF deployment will therefore inherit whatever DDOS protections are provided at the perimeter of the deployment.

Pivotal Cloud Foundry also supports the use of [Route Services](#), which can be used to add additional application-level (layer 7) protection.

In addition, PCF itself employs [rate limiting](#) techniques to protect against DOS attacks on, e.g. the Cloud Controller.

Control Description

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 references to sources for such information] by employing [Assignment: organization-defined security safeguards].

Supplemental Guidance

A variety of technologies exist to limit, or in some cases, eliminate the effects of denial of service attacks. For example, boundary protection devices can filter certain types of packets to protect information system components on internal organizational networks from being directly affected by denial of service attacks. Employing increased capacity and bandwidth combined with service redundancy may also reduce the susceptibility to denial of service attacks.

SC-6 RESOURCE AVAILABILITY

PCF Compliance

Not applicable. This control is classified as P0, and not required when operating at the FISMA Moderate level.

However, PCF PAS does comply with the intent of this control.

PCF PAS runs applications inside [linux containers](#) which provide a compliant level of resource isolation.

These linux containers are designed to provide isolation of application processes, including filesystem, network, memory, and CPU.

Control Description

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]].

Supplemental Guidance

Priority protection helps prevent lower-priority processes from delaying or interfering with the information system servicing any higher-priority processes. Quotas prevent users or processes from obtaining more than predetermined amounts of resources. This control does not apply to information system components for which there are only single users/roles.

SC-7 BOUNDARY PROTECTION

PCF Compliance

The PCF PAS [reference architecture](#) documents provide the technical guidance deployers need in order to satisfy any boundary protection requirements. When deployed in accordance with the recommended reference architecture, the PCF PAS deployment is compliant with this requirement.

For more information on the system boundaries of PCF see: <https://docs.pivotal.io/pivotalcf/concepts/security.html#system-boundaries>

Beyond the boundary protections provided by the IaaS network architecture, additional PAS flow control is provided using the following mechanisms:

a) Ingress to the platform is permitted only via the Cloud Foundry Router.

In addition, the Cloud Foundry Router provides [Route Services](#) which can be used to do application-level traffic shaping. The PAS inherits any network isolation protections defined by the IaaS administrator.

In addition, [Isolation Segments](#) can be used to separate workloads and thereby limit east-west traffic.

b) Egress from the platform is controlled by the use of Application Security Groups (ASG). For more information about ASGs, see [Understanding Application Security Groups](#).

c) Intra-platform application traffic may be controlled via container-to-container networking policies. These policies are default deny, with option for allowing connectivity between applications. For more information on C2C networking see [Understanding Container-to-Container Networking](#).

The Cloud Foundry Loggregator logging subsystem provides monitoring of all inbound and outbound network communications.

The deployer is responsible for ensuring that all connections to external third-party systems are done in accordance with the organization's approved security architecture.

Prevention of split tunnels from remote devices is out of scope for PCF and is a deployer responsibility.

Control Description

The information system:

- a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system;
- b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and
- c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

Supplemental Guidance

Managed interfaces include, for example, gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within a security architecture (e.g., routers protecting firewalls or application gateways residing on protected subnetworks). Subnetworks that are physically or logically separated from internal networks are referred to as demilitarized zones or DMZs. Restricting or prohibiting interfaces within organizational information systems includes, for example, restricting external web traffic to designated web servers within managed interfaces and prohibiting external traffic that appears to be spoofing internal addresses. Organizations consider the shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers, and may also include third party-provided access lines and other service elements. Such transmission services may represent sources of increased risk despite contract security provisions.

SC-8 TRANSMISSION CONFIDENTIALITY AND INTEGRITY

PCF Compliance

When deployed in accordance with the associate reference architecture, PCF PAS provides both confidentiality and integrity of transmitted information. All implied requirements are satisfied.

Network traffic to any PCF publicly accessible endpoint is protected via TLS, and optionally via SSH.

Network traffic within the PCF PAS private subnet may be protected using the IPsec BOSH Add-on.

For more information about IPsec see [IPsec Add-on for PCF](#).

For an overview of securing traffic into PCF see [Securing Traffic into Cloud Foundry](#).

For more information about TLS in PCF see [PCF Component and Container Security](#).

For more information about SSH in PCF see [Application SSH Overview](#) and [Configuring SSH Access for PCF](#).

For more information about SSH with BOSH see [Enabling SSH Access](#).

Control Description

The information system protects the [Selection (one or more): confidentiality; integrity] of transmitted information.

Supplemental Guidance

This control applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, facsimile machines). Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification. Protecting the confidentiality and/or integrity of organizational information can be accomplished by physical means (e.g., by employing protected distribution systems) or by logical means (e.g., employing encryption techniques). Organizations relying on commercial providers offering transmission services as commodity services rather than as fully dedicated services (i.e., services which can be highly specialized to individual customer needs), may find it difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission confidentiality/integrity. In such situations, organizations determine what types of confidentiality/integrity services are available in standard, commercial telecommunication service packages. If it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, organizations implement appropriate compensating security controls or explicitly accept the additional risk.

SC-9 TRANSMISSION CONFIDENTIALITY

PCF Compliance

Not applicable.

Control Description

[Withdrawn: Incorporated into SC-8].

Supplemental Guidance

SC-10 NETWORK DISCONNECT

PCF Compliance

As per the recommended reference architecture, PCF PAS is deployed behind an organization-managed load balancer. Deployers with a requirement to manage TCP session communications timeout settings must do so at the network level, via the Load Balancer management interface.

Native PCF PAS management API traffic, and any cloud native application traffic, both operate at level 7, over HTTP(S).

HTTP is stateless and user sessions are based on HTTP session headers, and the use of OAuth 2 tokens.

The OAuth 2 token lifetimes issued by UAA for use with Apps Manager, the CF CLI, and any application SSO can be configured to tailor the user login sessions appropriately.

For more information about HTTP routing and sessions in PCF PAS see [HTTP Routing](#).

For more information about customizing the Apps Manager and the cf CLI token lifetime see the [Configure UAA section](#) of [Deploying Elastic Runtime on AWS](#).

Control Description

The information system terminates the network connection associated with a communications session at the end of the session or after [Assignment: organization-defined time period] of inactivity.

Supplemental Guidance

This control applies to both internal and external networks. Terminating network connections associated with communications sessions include, for example, de-allocating associated TCP/IP address/port pairs at the operating system level, or de-allocating networking assignments at the application level if multiple application sessions are using a single, operating system-level network connection. Time periods of inactivity may be established by organizations and include, for example, time periods by type of network access or for specific network accesses.

SC-11 TRUSTED PATH

PCF Compliance

Not applicable.

Control Description

The information system establishes a trusted communications path between the user and the following security functions of the system: [Assignment: organization-defined security functions to include at a minimum, information system authentication and re-authentication].

Supplemental Guidance

Trusted paths are mechanisms by which users (through input devices) can communicate directly with security functions of information systems with the requisite assurance to support information security policies. The mechanisms can be activated only by users or the security functions of organizational information systems. User responses via trusted paths are protected from modifications by or disclosure to untrusted applications. Organizations employ trusted paths for high-assurance connections between security functions of information systems and users (e.g., during system logons). Enforcement of trusted communications paths is typically provided via an implementation that meets the reference monitor concept.

SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

PCF Compliance

It is a deployer responsibility to define all cryptographic key management policies and procedures. PCF satisfies all implied technical control requirements. For all PCF releases v1.12.0 and above, all certificates and keys in the environment can be rotated by the deployer, including the “non-configurable” certificates in Ops Manager. Procedures exist explaining how to rotate keys for Ops Manager and IPsec.

Rotation of the Cloud Controller mysql database key is supported in releases after v2.2.

More information on cryptographic key management is available on the following pages:

- [IPsec credential management](#) 
- [Ops Manager credential management](#) 
- [CredHub Overview](#) 
- [CredHub in PCF](#) 
- [CredHub for Tile Developers](#) 

Control Description

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].

Supplemental Guidance

Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures. Organizations define key management requirements in accordance with applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance, specifying appropriate options, levels, and parameters. Organizations manage trust stores to ensure that only approved trust anchors are in such trust stores. This includes certificates with visibility external to organizational information systems and certificates related to the internal operations of systems.

SC-13 CRYPTOGRAPHIC PROTECTION

PCF Compliance

Compliance with this requirement must be assessed with respect to each deployer's specific policy and procedure documents. In general, all implied requirements may be satisfied by an appropriate combination of PCF technical and organization-defined procedural controls.

Control Description

The information system implements [Assignment: organization-defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

Supplemental Guidance

Cryptography can be employed to support a variety of security solutions including, for example, the protection of classified and Controlled Unclassified Information, the provision of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearances for such information but lack the necessary formal access approvals. Cryptography can also be used to support random number generation and hash generation. Generally applicable cryptographic standards include FIPS-validated cryptography and NSA-approved cryptography. This control does not impose any requirements on organizations to use cryptography. However, if cryptography is required based on the selection of other security controls, organizations define each type of cryptographic use and the type of cryptography required (e.g., protection of classified information: NSA-approved cryptography; provision of digital signatures: FIPS-validated cryptography).

SC-14 PUBLIC ACCESS PROTECTIONS

PCF Compliance

Not applicable.

Control Description

[Withdrawn: Capability provided by AC-2, AC-3, AC-5, AC-6, SI-3, SI-4, SI-5, SI-7, SI-10].

Supplemental Guidance

SC-15 COLLABORATIVE COMPUTING DEVICES

PCF Compliance

Compliance with the requirements defined in this control is a deployer responsibility.

Interpretation of the requirement for notification of any remote session initiation in the PCF PAS operational environment might include the start of an SSH session.

When appropriately configured, an operator may know that someone has remotely connected via SSH to a VM or a container.

PCF provides audit logging for SSH session initiation and the deployer may establish a log alert to satisfy this requirement.

Control Description

The information system:

- a. Prohibits remote activation of collaborative computing devices with the following exceptions: [Assignment: organization-defined exceptions where remote activation is to be allowed]; and
- b. Provides an explicit indication of use to users physically present at the devices.

Supplemental Guidance

Collaborative computing devices include, for example, networked white boards, cameras, and microphones. Explicit indication of use includes, for example, signals to users when collaborative computing devices are activated.

SC-16 TRANSMISSION OF SECURITY ATTRIBUTES

PCF Compliance

This requirement is out of scope for PCF, and is the responsibility of the application developer. It is not required for systems operating at the FISMA moderate level.

Control Description

The information system associates [Assignment: organization-defined security attributes] with information exchanged between information systems and between system components.

Supplemental Guidance

Security attributes can be explicitly or implicitly associated with the information contained in organizational information systems or system components.

SC-17 PUBLIC KEY INFRASTRUCTURE CERTIFICATES

PCF Compliance

PCF PAS is compliant with all the technical controls stated or implied in this requirement.

For all but one function, PCF allows the deployer to supply enterprise-issued or enterprise-provisioned certificates. For the specific case of the “non-configurable” Ops Manager certificates, the deployer may not use their own CA but may rotate the internally generated certificates via an API.

For more information on Ops Manager certificate rotation see: <https://docs.pivotal.io/pivotalcf/security/pcf-infrastructure/api-cert-rotation.html> [↗](#)

For more information on configuring certificates for TLS termination at the CF router see: <https://docs.pivotal.io/pivotalcf/customizing/config-er-vmware.html#networking> [↗](#)

Certificates used by the IPsec BOSH Add-on are supplied by the deployer. For more information on IPsec certificate management see: <https://docs.pivotal.io/addon-ipsec/credentials.html> [↗](#)

Beginning with release version 2.0, PCF uses CredHub to manage all platform credentials. For more information on CredHub see:

- [Open Source CredHub documentation](#) [↗](#)
- [Pivotal CredHub documentation](#) [↗](#)

Control Description

The organization issues public key certificates under an [Assignment: organization-defined certificate policy] or obtains public key certificates from an approved service provider.

Supplemental Guidance

For all certificates, organizations manage information system trust stores to ensure only approved trust anchors are in the trust stores. This control addresses both certificates with visibility external to organizational information systems and certificates related to the internal operations of systems, for example, application-specific time services.

SC-18 MOBILE CODE

PCF Compliance

Compliance with the requirements defined in this control is a deployer responsibility.

All implied technical control requirements are satisfied by PCF.

Specifically, the use of buildpacks in PCF enables the operator to limit the use of, e.g. mobile code, through restrictions on developer access to an approved application stack.

Control Description

The organization:

- a. Defines acceptable and unacceptable mobile code and mobile code technologies;
- b. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and
- c. Authorizes, monitors, and controls the use of mobile code within the information system.

Supplemental Guidance

Decisions regarding the employment of mobile code within organizational information systems are based on the potential for the code to cause damage to the systems if used maliciously. Mobile code technologies include, for example, Java, JavaScript, ActiveX, Postscript, PDF, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidance apply to both the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations and devices (e.g., smart phones). Mobile code policy and procedures address preventing the development, acquisition, or introduction of unacceptable mobile code within organizational information systems.

SC-19 VOICE OVER INTERNET PROTOCOL

PCF Compliance

Compliance with the requirements defined in this control is a deployer responsibility.

Control Description

The organization:

- a. 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
- b. Authorizes, monitors, and controls the use of VoIP within the information system.

Supplemental Guidance

SC-20 SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)

PCF Compliance

This control implies a requirement for secure domain name resolution, such as via the use of, e.g., DNSSEC, though no specific implementation choice is mandated.

The interpretation of this control for PCF is that name resolution must be divided into two parts: external to PCF, and internal to PCF.

For name resolution of any endpoints that are external to PCF, such as the UAA or Cloud Controller, the FQDN should be resolved using a trusted DNS service.

That trust in DNS may be based upon runtime integrity checking using approved cryptographic mechanisms, such as via DNSSEC. Alternatively, trust in the DNS name resolution service used by PCF clients may be based upon a combination of appropriately securing the DNS client endpoint configuration, and appropriately restricting access to the enterprise DNS name server itself.

Regardless of the mechanism chosen, compliance with the requirement for name resolution external to the platform is a deployer responsibility.

Internal to PCF, the platform jobs and services rely upon the BOSH director to manage VM configuration and name resolution is done through BOSH DNS. In earlier PAS releases Consul and/or etcd provided the equivalent service location capabilities.

For more information on BOSH DNS see: <https://bosh.io/docs/dns/>

Name resolution for applications deployed to PAS containers is configured via Diego.

For more information about how containers perform DNS lookups on a Diego Cell, see [BOSH DNS Introduced Container DNS Behavior Changes in PAS 2.0](#) in the Pivotal [Knowledge Base].

Control Description

The information system:

- a. 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
- b. 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.

Supplemental Guidance

This control enables external clients including, for example, remote Internet clients, to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service. Information systems that provide name and address resolution services include, for example, domain name system (DNS) servers. Additional artifacts include, for example, DNS Security (DNSSEC) digital signatures and cryptographic keys. DNS resource records are examples of authoritative data. The means to indicate the security status of child zones includes, for example, the use of delegation signer resource records in the DNS. The DNS security controls reflect (and are referenced from) OMB Memorandum 08-23. Information systems that use technologies other than the DNS to map between host/service names and network addresses provide other means to assure the authenticity and integrity of response data.

SC-21 SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)

PCF Compliance

Address resolution for clients that need to reach endpoints at the external interface of PCF (such as applications hosted in PCF, or the UAA or Cloud Controller endpoint) are the responsibility of the deployer. The client will rely upon the DNS configuration of the endpoint device.

Address resolution internal to the PCF foundation is managed by BOSH DNS. As BOSH is responsible for assigning IP addresses for PCF platform jobs (BOSH releases), it also orchestrates name resolution for these addresses. Security of this name-to-address resolution is based on the trust relationship between the BOSH director and the BOSH agents. Address resolution for applications running within the PAS/ERT runtime container is delegated to the DNS specified by the operator, using the Ops Manager, or the IaaS supplied DNS.

See also the information provided for the related control [SC-20](#).

For more information on name resolution from containers, see [BOSH DNS Introduced Container DNS Behavior Changes in PAS 2.0](#) in the Pivotal Knowledge Base.

Control Description

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.

Supplemental Guidance

Each client of name resolution services either performs this validation on its own, or has authenticated channels to trusted validation providers. Information systems that provide name and address resolution services for local clients include, for example, recursive resolving or caching domain name system (DNS) servers. DNS client resolvers either perform validation of DNSSEC signatures, or clients use authenticated channels to recursive resolvers that perform such validations. Information systems that use technologies other than the DNS to map between host/service names and network addresses provide other means to enable clients to verify the authenticity and integrity of response data.

SC-22 ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE

PCF Compliance

External to the PCF system boundary, compliance with the requirements defined in this control is a deployer responsibility.

Internal to the PCF system boundary, BOSH DNS provides a trusted, highly available name resolution service that ensures PCF is compliant with this control.

Control Description

The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.

Supplemental Guidance

Information systems that provide name and address resolution services include, for example, domain name system (DNS) servers. To eliminate single points of failure and to enhance redundancy, organizations employ at least two authoritative domain name system servers, one configured as the primary server and the other configured as the secondary server. Additionally, organizations typically deploy the servers in two geographically separated network subnetworks (i.e., not located in the same physical facility). For role separation, DNS servers with internal roles only process name and address resolution requests from within organizations (i.e., from internal clients). DNS servers with external roles only process name and address resolution information requests from clients external to organizations (i.e., on external networks including the Internet). Organizations specify clients that can access authoritative DNS servers in particular roles (e.g., by address ranges, explicit lists).

SC-23 SESSION AUTHENTICITY

PCF Compliance

PCF is compliant with this control. PCF supports the use of TLS for all externally accessible entry points. OAuth 2 tokens are used for maintenance of Cloud Controller API sessions, and also to implement SSO to application instances.

Internal to the deployment, PCF uses both TLS and IPsec. For communications protected via IPsec, the IKEv2 protocol provides SA establishment. Authentication of IPsec peers is via X.509 certificates.

Direct operator access to a PCF VM host or application container is protected with the SSH protocol. SSH client authentication is implemented via a public/private key pair.

Control Description

The information system protects the authenticity of communications sessions.

Supplemental Guidance

This control addresses communications protection at the session, versus packet level (e.g., sessions in service-oriented architectures providing web-based services) and establishes grounds for confidence at both ends of communications sessions in ongoing identities of other parties and in the validity of information transmitted. Authenticity protection includes, for example, protecting against man-in-the-middle attacks/session hijacking and the insertion of false information into sessions.

SC-24 FAIL IN KNOWN STATE

PCF Compliance

Not applicable.

Control Description

The information system fails to a [Assignment: organization-defined known-state] for [Assignment: organization-defined types of failures] preserving [Assignment: organization-defined system state information] in failure.

Supplemental Guidance

Failure in a known state addresses security concerns in accordance with the mission/business needs of organizations. Failure in a known secure state helps to prevent the loss of confidentiality, integrity, or availability of information in the event of failures of organizational information systems or system components. Failure in a known safe state helps to prevent systems from failing to a state that may cause injury to individuals or destruction to property. Preserving information system state information facilitates system restart and return to the operational mode of organizations with less disruption of mission/business processes.

SC-25 THIN NODES

PCF Compliance

Not applicable.

Control Description

The organization employs [Assignment: organization-defined information system components] with minimal functionality and information storage.

Supplemental Guidance

The deployment of information system components with reduced/minimal functionality (e.g., diskless nodes and thin client technologies) reduces the need to secure every user endpoint, and may reduce the exposure of information, information systems, and services to cyber attacks.

SC-26 HONEYPOTS

PCF Compliance

Not applicable.

Control Description

The information system includes components specifically designed to be the target of malicious attacks for the purpose of detecting, deflecting, and analyzing such attacks.

Supplemental Guidance

A honeypot is set up as a decoy to attract adversaries and to deflect their attacks away from the operational systems supporting organizational missions/business function. Depending upon the specific usage of the honeypot, consultation with the Office of the General Counsel before deployment may be needed.

SC-27 PLATFORM-INDEPENDENT APPLICATIONS

PCF Compliance

Not applicable.

Control Description

The information system includes: [Assignment: organization-defined platform-independent applications].

Supplemental Guidance

Platforms are combinations of hardware and software used to run software applications. Platforms include: (i) operating systems; (ii) the underlying computer architectures, or (iii) both. Platform-independent applications are applications that run on multiple platforms. Such applications promote portability and reconstitution on different platforms, increasing the availability of critical functions within organizations while information systems with specific operating systems are under attack.

SC-28 PROTECTION OF INFORMATION AT REST

PCF Compliance

PCF is compatible with the use of IaaS-provided data-at-rest disk encryption when this capability is available. It is an operator responsibility to appropriately configure the deployment.

Integration of PCF and Ops Manager with a native IaaS-provided key management service may vary by IaaS.

Operators can specify a custom AWS Key Management Service (KMS) encryption key to encrypt all the Elastic Block Store (EBS) volumes in AWS for BOSH VMs and the Ops Manager VM.

For more information about PCF integration with IaaS disk encryption capabilities see:

- <https://docs.pivotal.io/pivotalcf/customizing/cloudform-om-ebs-config.html> [↗](#)
- <https://docs.pivotal.io/pivotalcf/installing/highlights.html#custom-kms> [↗](#)
- <https://docs.pivotal.io/pivotalcf/installing/highlights.html#blobstore-encryption> [↗](#)

In addition, PCF also encrypts sensitive information in the Cloud Controller database explicitly. Key material for this protection is auto-generated uniquely for each deployment.

Control Description

The information system protects the [Selection (one or more): confidentiality; integrity] of [Assignment: organization-defined information at rest].

Supplemental Guidance

This control addresses the confidentiality and integrity of information at rest and covers user information and system information. Information at rest refers to the state of information when it is located on storage devices as specific components of information systems. System-related information requiring protection includes, for example, configurations or rule sets for firewalls, gateways, intrusion detection/prevention systems, filtering routers, and authenticator content. Organizations may employ different mechanisms to achieve confidentiality and integrity protections, including the use of cryptographic mechanisms and file share scanning. Integrity protection can be achieved, for example, by implementing Write-Once-Read-Many (WORM) technologies. Organizations may also employ other security controls including, for example, secure off-line storage in lieu of online storage when adequate protection of information at rest cannot otherwise be achieved and/or continuous monitoring to identify malicious code at rest.

SC-29 HETEROGENEITY

PCF Compliance

Not applicable.

Control Description

The organization employs a diverse set of information technologies for [Assignment: organization-defined information system components] in the implementation of the information system.

Supplemental Guidance

Increasing the diversity of information technologies within organizational information systems reduces the impact of potential exploitations of specific technologies and also defends against common mode failures, including those failures induced by supply chain attacks. Diversity in information technologies also reduces the likelihood that the means adversaries use to compromise one information system component will be equally effective against other system components, thus further increasing the adversary work factor to successfully complete planned cyber attacks. An increase in diversity may add complexity and management overhead which could ultimately lead to mistakes and unauthorized configurations.

SC-30 CONCEALMENT AND MISDIRECTION

PCF Compliance

Not applicable.

Control Description

The organization employs [Assignment: organization-defined concealment and misdirection techniques] for [Assignment: organization-defined information systems] at [Assignment: organization-defined time periods] to confuse and mislead adversaries.

Supplemental Guidance

Concealment and misdirection techniques can significantly reduce the targeting capability of adversaries (i.e., window of opportunity and available attack surface) to initiate and complete cyber attacks. For example, virtualization techniques provide organizations with the ability to disguise information systems, potentially reducing the likelihood of successful attacks without the cost of having multiple platforms. Increased use of concealment/misdirection techniques including, for example, randomness, uncertainty, and virtualization, may sufficiently confuse and mislead adversaries and subsequently increase the risk of discovery and/or exposing tradecraft. Concealment/misdirection techniques may also provide organizations additional time to successfully perform core missions and business functions. Because of the time and effort required to support concealment/misdirection techniques, it is anticipated that such techniques would be used by organizations on a very limited basis.

SC-31 COVERT CHANNEL ANALYSIS

PCF Compliance

Not applicable.

Control Description

The organization:

- a. Performs a covert channel analysis to identify those aspects of communications within the information system that are potential avenues for covert [Selection (one or more): storage; timing] channels; and
- b. Estimates the maximum bandwidth of those channels.

Supplemental Guidance

Developers are in the best position to identify potential areas within systems that might lead to covert channels. Covert channel analysis is a meaningful activity when there is the potential for unauthorized information flows across security domains, for example, in the case of information systems containing export-controlled information and having connections to external networks (i.e., networks not controlled by organizations). Covert channel analysis is also meaningful for multilevel secure (MLS) information systems, multiple security level (MSL) systems, and cross-domain systems.

SC-32 INFORMATION SYSTEM PARTITIONING

PCF Compliance

Not applicable.

Control Description

The organization partitions the information system into [Assignment: organization-defined information system components] residing in separate physical domains or environments based on [Assignment: organization-defined circumstances for physical separation of components].

Supplemental Guidance

Information system partitioning is a part of a defense-in-depth protection strategy. Organizations determine the degree of physical separation of system components from physically distinct components in separate racks in the same room, to components in separate rooms for the more critical components, to more significant geographical separation of the most critical components. Security categorization can guide the selection of appropriate candidates for domain partitioning. Managed interfaces restrict or prohibit network access and information flow among partitioned information system components.

SC-33 TRANSMISSION PREPARATION INTEGRITY

PCF Compliance

Not applicable.

Control Description

[Withdrawn: Incorporated into SC-8].

Supplemental Guidance

SC-34 NON-MODIFIABLE EXECUTABLE PROGRAMS

PCF Compliance

Not applicable.

Control Description

The information system at [Assignment: organization-defined information system components]:

- a. Loads and executes the operating environment from hardware-enforced, read-only media; and
- b. Loads and executes [Assignment: organization-defined applications] from hardware-enforced, read-only media.

Supplemental Guidance

The term operating environment is defined as the specific code that hosts applications, for example, operating systems, executives, or monitors including virtual machine monitors (i.e., hypervisors). It can also include certain applications running directly on hardware platforms. Hardware-enforced, read-only media include, for example, Compact Disk-Recordable (CD-R)/Digital Video Disk-Recordable (DVD-R) disk drives and one-time programmable read-only memory. The use of non-modifiable storage ensures the integrity of software from the point of creation of the read-only image. The use of reprogrammable read-only memory can be accepted as read-only media provided: (i) integrity can be adequately protected from the point of initial writing to the insertion of the memory into the information system; and (ii) there are reliable hardware protections against reprogramming the memory while installed in organizational information systems.

SC-35 HONEYCLIENTS

PCF Compliance

Not applicable.

Control Description

The information system includes components that proactively seek to identify malicious websites and/or web-based malicious code.

Supplemental Guidance

Honeyclients differ from honeypots in that the components actively probe the Internet in search of malicious code (e.g., worms) contained on external websites. As with honeypots, honeyclients require some supporting isolation measures (e.g., virtualization) to ensure that any malicious code discovered during the search and subsequently executed does not infect organizational information systems.

SC-36 DISTRIBUTED PROCESSING AND STORAGE

PCF Compliance

Not applicable.

Control Description

The organization distributes [Assignment: organization-defined processing and storage] across multiple physical locations.

Supplemental Guidance

Distributing processing and storage across multiple physical locations provides some degree of redundancy or overlap for organizations, and therefore increases the work factor of adversaries to adversely impact organizational operations, assets, and individuals. This control does not assume a single primary processing or storage location, and thus allows for parallel processing and storage.

SC-37 OUT-OF-BAND CHANNELS

PCF Compliance

Not applicable.

Control Description

The organization employs [Assignment: organization-defined out-of-band channels] for the physical delivery or electronic transmission of [Assignment: organization-defined information, information system components, or devices] to [Assignment: organization-defined individuals or information systems].

Supplemental Guidance

Out-of-band channels include, for example, local (nonnetwork) accesses to information systems, network paths physically separate from network paths used for operational traffic, or nonelectronic paths such as the US Postal Service. This is in contrast with using the same channels (i.e., in-band channels) that carry routine operational traffic. Out-of-band channels do not have the same vulnerability/exposure as in-band channels, and hence the confidentiality, integrity, or availability compromises of in-band channels will not compromise the out-of-band channels. Organizations may employ out-of-band channels in the delivery or transmission of many organizational items including, for example, identifiers/authenticators, configuration management changes for hardware, firmware, or software, cryptographic key management information, security updates, system/data backups, maintenance information, and malicious code protection updates.

SC-38 OPERATIONS SECURITY

PCF Compliance

Not applicable.

Control Description

The organization employs [Assignment: organization-defined operations security safeguards] to protect key organizational information throughout the system development life cycle.

Supplemental Guidance

Operations security (OPSEC) is a systematic process by which potential adversaries can be denied information about the capabilities and intentions of organizations by identifying, controlling, and protecting generally unclassified information that specifically relates to the planning and execution of sensitive organizational activities. The OPSEC process involves five steps: (i) identification of critical information (e.g., the security categorization process); (ii) analysis of threats; (iii) analysis of vulnerabilities; (iv) assessment of risks; and (v) the application of appropriate countermeasures. OPSEC safeguards are applied to both organizational information systems and the environments in which those systems operate. OPSEC safeguards help to protect the confidentiality of key information including, for example, limiting the sharing of information with suppliers and potential suppliers of information system components, information technology products and services, and with other non-organizational elements and individuals.

Information critical to mission/business success includes, for example, user identities, element uses, suppliers, supply chain processes, functional and security requirements, system design specifications, testing protocols, and security control implementation details.

SC-39 PROCESS ISOLATION

PCF Compliance

PCF is compliant with the technical controls implied by this control. Applications deployed to PCF are isolated from each other through the use of linux containers in the environment.

For more information on container security see: <https://docs.pivotal.io/pivotalcf/concepts/container-security.html> 

Control Description

The information system maintains a separate execution domain for each executing process.

Supplemental Guidance

Information systems can maintain separate execution domains for each executing process by assigning each process a separate address space. Each information system process has a distinct address space so that communication between processes is performed in a manner controlled through the security functions, and one process cannot modify the executing code of another process. Maintaining separate execution domains for executing processes can be achieved, for example, by implementing separate address spaces. This capability is available in most commercial operating systems that employ multi-state processor technologies.

SC-40 WIRELESS LINK PROTECTION

PCF Compliance

Not applicable.

Control Description

The information system protects external and internal [Assignment: organization-defined wireless links] from [Assignment: organization-defined types of signal parameter attacks or references to sources for such attacks].

Supplemental Guidance

This control applies to internal and external wireless communication links that may be visible to individuals who are not authorized information system users. Adversaries can exploit the signal parameters of wireless links if such links are not adequately protected. There are many ways to exploit the signal parameters of wireless links to gain intelligence, deny service, or to spoof users of organizational information systems. This control reduces the impact of attacks that are unique to wireless systems. If organizations rely on commercial service providers for transmission services as commodity items rather than as fully dedicated services, it may not be possible to implement this control.

SC-41 PORT AND I/O DEVICE ACCESS

PCF Compliance

Not applicable.

Control Description

The organization physically disables or removes [Assignment: organization-defined connection ports or input/output devices] on [Assignment: organization-defined information systems or information system components].

Supplemental Guidance

Connection ports include, for example, Universal Serial Bus (USB) and Firewire (IEEE 1394). Input/output (I/O) devices include, for example, Compact Disk (CD) and Digital Video Disk (DVD) drives. Physically disabling or removing such connection ports and I/O devices helps prevent exfiltration of information from information systems and the introduction of malicious code into systems from those ports/devices.

SC-42 SENSOR CAPABILITY AND DATA

PCF Compliance

Not applicable.

Control Description

The information system:

- a. Prohibits the remote activation of environmental sensing capabilities with the following exceptions: [Assignment: organization-defined exceptions where remote activation of sensors is allowed]; and
- b. Provides an explicit indication of sensor use to [Assignment: organization-defined class of users].

Supplemental Guidance

This control often applies to types of information systems or system components characterized as mobile devices, for example, smart phones, tablets, and E-readers. These systems often include sensors that can collect and record data regarding the environment where the system is in use. Sensors that are embedded within mobile devices include, for example, cameras, microphones, Global Positioning System (GPS) mechanisms, and accelerometers. While the sensors on mobile devices provide an important function, if activated covertly, such devices can potentially provide a means for adversaries to learn valuable information about individuals and organizations. For example, remotely activating the GPS function on a mobile device could provide an adversary with the ability to track the specific movements of an individual.

SC-43 USAGE RESTRICTIONS

PCF Compliance

Not applicable.

Control Description

The organization:

- a. Establishes usage restrictions and implementation guidance for [Assignment: organization-defined information system components] based on the potential to cause damage to the information system if used maliciously; and
- b. Authorizes, monitors, and controls the use of such components within the information system.

Supplemental Guidance

Information system components include hardware, software, or firmware components (e.g., Voice Over Internet Protocol, mobile code, digital copiers, printers, scanners, optical devices, wireless technologies, mobile devices).

SC-44 DETONATION CHAMBERS

PCF Compliance

Not applicable.

Control Description

The organization employs a detonation chamber capability within [Assignment: organization-defined information system, system component, or location].

Supplemental Guidance

Detonation chambers, also known as dynamic execution environments, allow organizations to open email attachments, execute untrusted or suspicious applications, and execute Universal Resource Locator (URL) requests in the safety of an isolated environment or virtualized sandbox. These protected and isolated execution environments provide a means of determining whether the associated attachments/applications contain malicious code. While related to the concept of deception nets, the control is not intended to maintain a long-term environment in which adversaries can operate and their actions can be observed. Rather, it is intended to quickly identify malicious code and reduce the likelihood that the code is propagated to user environments of operation (or prevent such propagation completely).

System And Information Integrity Control Family

Number	Control	Pivotal Application Service (PAS) Compliance
SI-1	SI-1 SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES	Inherited
SI-2	FLAW REMEDIATION	Inherited and Compliant
SI-3	MALICIOUS CODE PROTECTION	Inherited and Compliant
SI-4	INFORMATION SYSTEM MONITORING	Inherited and Compliant
SI-5	SECURITY ALERTS, ADVISORIES, AND DIRECTIVES	Inherited and Compliant
SI-6	SECURITY FUNCTION VERIFICATION	P0, so not required for FISMA Moderate
SI-7	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY	Inherited and Compliant
SI-8	SPAM PROTECTION	Inherited
SI-9	INFORMATION INPUT RESTRICTIONS	Not Applicable to PCF
SI-10	INFORMATION INPUT VALIDATION	Inherited and Compliant
SI-11	ERROR HANDLING	Inherited and Compliant
SI-12	INFORMATION HANDLING AND RETENTION	Inherited
SI-13	PREDICTABLE FAILURE PREVENTION	P0, so not required for FISMA Moderate
SI-14	NON-PERSISTENCE	P0, so not required for FISMA Moderate
SI-15	INFORMATION OUTPUT FILTERING	P0, so not required for FISMA Moderate
SI-16	MEMORY PROTECTION	Compliant
SI-17	FAIL-SAFE PROCEDURES	P0, so not required for FISMA Moderate

SI-1 SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES

PCF Compliance

All dash-1 requirements are the responsibility of the deployer. Pivotal may be able to provide guidance to customers who are creating or updating documentation, but this documentation is unique to the deployer's mission and business goals. All implied requirements are satisfied. PCF features are sufficient to satisfy SI-1.

Control Description

The organization:

- a. 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
- b. Reviews and updates the current:
 1. System and information integrity policy [Assignment: organization-defined frequency]; and
 2. System and information integrity procedures [Assignment: organization-defined frequency].

Supplemental Guidance

This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the SI family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

SI-2 FLAW REMEDIATION

PCF Compliance

PCF is compliant with this requirement. Pivotal regularly publishes security updates for Pivotal Cloud Foundry on [Pivotal Network](#). Operators may subscribe to update notifications from [Pivotal Network](#) and use BOSH and Ops Manager to keep their deployments up-to-date.

When an operator applies a patch, PCF systematically rolls the update out to all VMs in a deployment, avoiding the need to patch individual VMs.

Pivotal provides the following incident response support resources:

- RSS feed of Pivotal vulnerability reports: <https://pivotal.io/security/rss>
- Pivotal Product Vulnerability Reports, archived on the Pivotal Application Security Team website: <https://pivotal.io/security>

See [Security Processes and Stemcells](#) in the PCF documentation for more information.

The PCF deployer is responsible for performing scans for both configuration and vulnerabilities. PCF supports the use of third-party scanners, either through remote access scanning, or through local installation of third-party agents on the BOSH stemcells.

PCF deployers performing configuration scans against a PCF deployment should adjust their scanning benchmark to perform a cloud-native assessment, as opposed to employing a scanning benchmark intended for standalone Linux server deployments.

PCF deployers requiring assistance with scanning a deployment can contact the Pivotal Security team at security@pivotal.io.

Control Description

The organization:

- a. Identifies, reports, and corrects information system flaws;
- b. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
- c. Installs security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the updates; and
- d. Incorporates flaw remediation into the organizational configuration management process.

Supplemental Guidance

Organizations identify information systems affected by announced software flaws including potential vulnerabilities resulting from those flaws, and report this information to designated organizational personnel with information security responsibilities. Security-relevant software updates include, for example, patches, service packs, hot fixes, and anti-virus signatures. Organizations also address flaws discovered during security assessments, continuous monitoring, incident response activities, and system error handling. Organizations take advantage of available resources such as the Common Weakness Enumeration (CWE) or Common Vulnerabilities and Exposures (CVE) databases in remediating flaws discovered in organizational information systems. By incorporating flaw remediation into ongoing configuration management processes, required/anticipated remediation actions can be tracked and verified. Flaw remediation actions that can be tracked and verified include, for example, determining whether organizations follow US-CERT guidance and Information Assurance Vulnerability Alerts. Organization-defined time periods for updating security-relevant software and firmware may vary based on a variety of factors including, for example, the security category of the information system or the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw). Some types of flaw remediation may require more testing than other types. Organizations determine the degree and type of testing needed for the specific type of flaw remediation activity under consideration and also the types of changes that are to be configuration-managed. In some situations, organizations may determine that the testing of software and/or firmware updates is not necessary or practical, for example, when implementing simple anti-virus signature updates. Organizations may also consider in testing decisions, whether security-relevant software or firmware updates are obtained from authorized sources with appropriate digital signatures.

SI-3 MALICIOUS CODE PROTECTION

PCF Compliance

Compliance with this requirement is primarily a deployer responsibility. PCF supports the use of antivirus and file integrity monitoring through the following BOSH add-ons:

- [ClamAV Add-on for PCF](#) 
- [File Integrity Monitoring Add-on for PCF](#) 

The following additional resources are available to help PCF deployers with malicious code protection on the PCF platform:

- [BOSH Director Runtime Config](#) 
- [BOSH Linux OS Configuration Release](#) 

Control Description

The organization:

- a. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code;
- b. Updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures;
- c. Configures malicious code protection mechanisms to:
 1. Perform periodic scans of the information system [Assignment: organization-defined frequency] and real-time scans of files from external sources at [Selection (one or more); endpoint; network entry/exit points] as the files are downloaded, opened, or executed in accordance with organizational security policy; and
 2. [Selection (one or more): block malicious code; quarantine malicious code; send alert to administrator; [Assignment: organization-defined action]] in response to malicious code detection; and
- d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system

Supplemental Guidance

Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, notebook computers, and mobile devices. Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats (e.g., UUENCODE, Unicode), contained within compressed or hidden files, or hidden in files using steganography. Malicious code can be transported by different means including, for example, web accesses, electronic mail, electronic mail attachments, and portable storage devices. Malicious code insertions occur through the exploitation of information system vulnerabilities. Malicious code protection mechanisms include, for example, anti-virus signature definitions and reputation-based technologies. A variety of technologies and methods exist to limit or eliminate the effects of malicious code. Pervasive configuration management and comprehensive software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include, for example, logic bombs, back doors, and other types of cyber attacks that could affect organizational missions/business functions. Traditional malicious code protection mechanisms cannot always detect such code. In these situations, organizations rely instead on other safeguards including, for example, secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to help ensure that software does not perform functions other than the functions intended. Organizations may determine that in response to the detection of malicious code, different actions may be warranted. For example, organizations can define actions in response to malicious code detection during periodic scans, actions in response to detection of malicious downloads, and/or actions in response to detection of maliciousness when attempting to open or execute files.

SI-4 INFORMATION SYSTEM MONITORING

PCF Compliance

PCF is compliant with this requirement. The PCF deployer is responsible for information system monitoring, which can include system component monitoring via syslog and application monitoring through the Loggregator Firehose component. All PCF platform logging and monitoring may be forwarded to a syslog drain that performs alerting as needed. See [Configuring Logging in PAS](#) for more information.

PCF supports third-party security scanning, either through remote access, or through local installation of a third-party agent on the stemcell as a BOSH add-on.

PCF deployers requiring assistance configuring information system monitoring can contact the Pivotal Security team at security@pivotal.io.

Control Description

The organization:

- a. 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;
- b. Identifies unauthorized use of the information system through [Assignment: organization-defined techniques and methods];
- c. Deploys monitoring devices:
 1. Strategically within the information system to collect organization-determined essential information; and
 2. At ad hoc locations within the system to track specific types of transactions of interest to the organization;
- d. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;
- e. 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;
- f. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and
- g. 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]].

Supplemental Guidance

Information system monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at the information system boundary (i.e., part of perimeter defense and boundary protection). Internal monitoring includes the observation of events occurring within the information system. Organizations can monitor information systems, for example, by observing audit activities in real time or by observing other system aspects such as access patterns, characteristics of access, and other actions. The monitoring objectives may guide determination of the events. Information system monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, scanning tools, audit record monitoring software, network monitoring software). Strategic locations for monitoring devices include, for example, selected perimeter locations and near server farms supporting critical applications, with such devices typically being employed at the managed interfaces associated with controls SC-7 and AC-17. Einstein network monitoring devices from the Department of Homeland Security can also be included as monitoring devices. The granularity of monitoring information collected is based on organizational monitoring objectives and the capability of information systems to support such objectives. Specific types of transactions of interest include, for example, Hyper Text Transfer Protocol (HTTP) traffic that bypasses HTTP proxies. Information system monitoring is an integral part of organizational continuous monitoring and incident response programs. Output from system monitoring serves as input to continuous monitoring and incident response programs. A network connection is any connection with a device that communicates through a network (e.g., local area network, Internet). A remote connection is any connection with a device communicating through an external network (e.g., the Internet). Local, network, and remote connections can be either wired or wireless.

SI-5 SECURITY ALERTS, ADVISORIES, AND DIRECTIVES

PCF Compliance

PCF delegates responsibility for security alerts to the existing enterprise log management system. When appropriately configured, PCF forwards all activity logging to the designated enterprise log management system, and alerts or triggers for specific events may be established there. All implied requirements for this requirement are satisfied by the PCF platform.

Control Description

The organization:

- a. Receives information system security alerts, advisories, and directives from [Assignment: organization-defined external organizations] on an ongoing basis;
- b. Generates internal security alerts, advisories, and directives as deemed necessary;
- c. Disseminates security alerts, advisories, and directives to: [Selection (one or more): [Assignment: organization-defined personnel or roles]; [Assignment: organization-defined elements within the organization]; [Assignment: organization-defined external organizations]]; and
- d. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.

Supplemental Guidance

The United States Computer Emergency Readiness Team (US-CERT) generates security alerts and advisories to maintain situational awareness across the federal government. Security directives are issued by OMB or other designated organizations with the responsibility and authority to issue such directives. Compliance to security directives is essential due to the critical nature of many of these directives and the potential immediate adverse effects on organizational operations and assets, individuals, other organizations, and the Nation should the directives not be implemented in a timely manner. External organizations include, for example, external mission/business partners, supply chain partners, external service providers, and other peer/supporting organizations.

SI-6 SECURITY FUNCTION VERIFICATION

PCF Compliance

P0, so not required for [FISMA](#) Moderate.

Control Description

The information system:

- a. Verifies the correct operation of [Assignment: organization-defined security functions];
- b. Performs this verification [Selection (one or more): [Assignment: organization-defined system transitional states]; upon command by user with appropriate privilege; [Assignment: organization-defined frequency]];
- c. Notifies [Assignment: organization-defined personnel or roles] of failed security verification tests; and
- d. [Selection (one or more): shuts the information system down; restarts the information system; [Assignment: organization-defined alternative action(s)]] when anomalies are discovered.

Supplemental Guidance

Transitional states for information systems include, for example, system startup, restart, shutdown, and abort. Notifications provided by information systems include, for example, electronic alerts to system administrators, messages to local computer consoles, and/or hardware indications such as lights.

SI-7 SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY

PCF Compliance

PCF is compliant with this requirement.

The [File Integrity Monitoring](#) add-on for PCF monitors file integrity for all BOSH-deployed VMs.

By default, all BOSH-deployed VMs run the Linux audit daemon. Operators can edit their BOSH [runtime config](#) to customize the audit daemon and other native Linux auditing tools.

PCF supports third-party security scanning, either through remote access, or through local installation of a third-party agent on the stemcell as a BOSH add-on.

[Pivotal Network](#) provides checksums for all software releases, enabling deployers to check file integrity before deployment. In the future, Pivotal plans to add digital signatures to releases on Pivotal Network.

PCF deployers requiring assistance configuring integrity verification can contact the Pivotal Security team at security@pivotal.io.

Control Description

The organization employs integrity verification tools to detect unauthorized changes to [Assignment: organization-defined software, firmware, and information].

Supplemental Guidance

Unauthorized changes to software, firmware, and information can occur due to errors or malicious activity (e.g., tampering). Software includes, for example, operating systems (with key internal components such as kernels, drivers), middleware, and applications. Firmware includes, for example, the Basic Input Output System (BIOS). Information includes metadata such as security attributes associated with information. State-of-the-practice integrity-checking mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and associated tools can automatically monitor the integrity of information systems and hosted applications.

SI-8 SPAM PROTECTION

PCF Compliance

Compliance with this requirement is the responsibility of the PCF deployer.

Control Description

The organization:

- a. Employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages; and
- b. Updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.

Supplemental Guidance

Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, mobile devices, and notebook/laptop computers. Spam can be transported by different means including, for example, electronic mail, electronic mail attachments, and web accesses. Spam protection mechanisms include, for example, signature definitions.

SI-9 INFORMATION INPUT RESTRICTIONS

PCF Compliance

This control is not applicable to PCF.

Control Description

[Withdrawn: Incorporated into AC-2, AC-3, AC-5, AC-6].

Supplemental Guidance

SI-10 INFORMATION INPUT VALIDATION

PCF Compliance

PCF is compliant with this requirement. Pivotal performs penetration testing on all user interfaces and system entry points.

Information input validation for applications is the responsibility of the application developer.

Control Description

The information system checks the validity of [Assignment: organization-defined information inputs].

Supplemental Guidance

Checking the valid syntax and semantics of information system inputs (e.g., character set, length, numerical range, and acceptable values) verifies that inputs match specified definitions for format and content. Software applications typically follow well-defined protocols that use structured messages (i.e., commands or queries) to communicate between software modules or system components. Structured messages can contain raw or unstructured data interspersed with metadata or control information. If software applications use attacker-supplied inputs to construct structured messages without properly encoding such messages, then the attacker could insert malicious commands or special characters that can cause the data to be interpreted as control information or metadata. Consequently, the module or component that receives the tainted output will perform the wrong operations or otherwise interpret the data incorrectly. Prescreening inputs prior to passing to interpreters prevents the content from being unintentionally interpreted as commands. Input validation helps to ensure accurate and correct inputs and prevent attacks such as cross-site scripting and a variety of injection attacks.

SI-11 ERROR HANDLING

PCF Compliance

PCF is compliant with this requirement.

Errors returned from PCF APIs and UIs contain enough information to determine the nature of the problem, but do not disclose inappropriate information such as passwords. System logs that stream to a syslog endpoint are similarly designed to not avoid disclosing sensitive information to an unauthorized listener.

Application code is the deployer's responsibility. Authorization to see application logs may be controlled by the Cloud Controller RBAC restrictions, which are scoped by Org and Space abstractions.

The deployer may use a [nozzle](#) to direct log streams from the Firehose to secure drains. The deployer may also use authorization controls present in their third-party log management system to control access to archival logs.

The BOSH Director, Ops Manager, and other PCF system components also stream component logs via syslog. Deployers may restrict these logs to specific personnel based on their source.

Control Description

The information system:

- a. Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries; and
- b. Reveals error messages only to [Assignment: organization-defined personnel or roles].

Supplemental Guidance

Organizations carefully consider the structure/content of error messages. The extent to which information systems are able to identify and handle error conditions is guided by organizational policy and operational requirements. Information that could be exploited by adversaries includes, for example, erroneous logon attempts with passwords entered by mistake as the username, mission/business information that can be derived from (if not stated explicitly by) information recorded, and personal information such as account numbers, social security numbers, and credit card numbers. In addition, error messages may provide a covert channel for transmitting information.

SI-12 INFORMATION HANDLING AND RETENTION

PCF Compliance

Compliance with this requirement is the responsibility of the PCF deployer.

Control Description

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.

Supplemental Guidance

Information handling and retention requirements cover the full life cycle of information, in some cases extending beyond the disposal of information systems. The National Archives and Records Administration provides guidance on records retention.

SI-13 PREDICTABLE FAILURE PREVENTION

PCF Compliance

P0, so not required for [FISMA](#) Moderate.

Control Description

The organization:

- a. Determines mean time to failure (MTTF) for [Assignment: organization-defined information system components] in specific environments of operation; and
- b. Provides substitute information system components and a means to exchange active and standby components at [Assignment: organization-defined MTTF substitution criteria].

Supplemental Guidance

While MTTF is primarily a reliability issue, this control addresses potential failures of specific information system components that provide security capability. Failure rates reflect installation-specific consideration, not industry-average. Organizations define criteria for substitution of information system components based on MTTF value with consideration for resulting potential harm from component failures. Transfer of responsibilities between active and standby components does not compromise safety, operational readiness, or security capability (e.g., preservation of state variables). Standby components remain available at all times except for maintenance issues or recovery failures in progress.

SI-14 NON-PERSISTENCE

PCF Compliance

P0, so not required for [FISMA](#) Moderate.

Control Description

The organization implements non-persistent [Assignment: organization-defined information system components and services] that are initiated in a known state and terminated [Selection (one or more): upon end of session of use; periodically at [Assignment: organization-defined frequency]].

Supplemental Guidance

This control mitigates risk from advanced persistent threats (APTs) by significantly reducing the targeting capability of adversaries (i.e., window of opportunity and available attack surface) to initiate and complete cyber attacks. By implementing the concept of non-persistence for selected information system components, organizations can provide a known state computing resource for a specific period of time that does not give adversaries sufficient time on target to exploit vulnerabilities in organizational information systems and the environments in which those systems operate. Since the advanced persistent threat is a high-end threat with regard to capability, intent, and targeting, organizations assume that over an extended period of time, a percentage of cyber attacks will be successful. Non-persistent information system components and services are activated as required using protected information and terminated periodically or upon the end of sessions. Non-persistence increases the work factor of adversaries in attempting to compromise or breach organizational information systems. Non-persistent system components can be implemented, for example, by periodically re-imaging components or by using a variety of common virtualization techniques. Non-persistent services can be implemented using virtualization techniques as part of virtual machines or as new instances of processes on physical machines (either persistent or non-persistent). The benefit of periodic refreshes of information system components/services is that it does not require organizations to first determine whether compromises of components or services have occurred (something that may often be difficult for organizations to determine). The refresh of selected information system components and services occurs with sufficient frequency to prevent the spread or intended impact of attacks, but not with such frequency that it makes the information system unstable. In some instances, refreshes of critical components and services may be done periodically in order to hinder the ability of adversaries to exploit optimum windows of vulnerabilities.

SI-15 INFORMATION OUTPUT FILTERING

PCF Compliance

P0, so not required for [FISMA](#) Moderate.

Control Description

The information system validates information output from [Assignment: organization-defined software programs and/or applications] to ensure that the information is consistent with the expected content.

Supplemental Guidance

Certain types of cyber attacks (e.g., SQL injections) produce output results that are unexpected or inconsistent with the output results that would normally be expected from software programs or applications. This control enhancement focuses on detecting extraneous content, preventing such extraneous content from being displayed, and alerting monitoring tools that anomalous behavior has been discovered.

SI-16 MEMORY PROTECTION

PCF Compliance

The PCF product feature set is sufficient to satisfy the technical requirements implied in SI-16. Each instance of an app deployed to PCF runs within its own container, a self-contained environment. This container isolates processes, memory, and the filesystem using operating system features and the characteristics of the virtual and physical infrastructure where PCF is deployed.

PCF stemcells follow industry-standard hardening guidance and maintain a secure posture by default. For example, PCF is preconfigured to randomize address space layout and restrict file system mount options such as `noexec` and `read-only`.

For more information, see [Understanding Container Security](#).

Control Description

The information system implements [Assignment: organization-defined security safeguards] to protect its memory from unauthorized code execution.

Supplemental Guidance

Some adversaries launch attacks with the intent of executing code in non-executable regions of memory or in memory locations that are prohibited. Security safeguards employed to protect memory include, for example, data execution prevention and address space layout randomization. Data execution prevention safeguards can either be hardware-enforced or software-enforced with hardware providing the greater strength of mechanism.

SI-17 FAIL-SAFE PROCEDURES

PCF Compliance

P0, so not required for [FISMA](#) Moderate.

Control Description

The information system implements [Assignment: organization-defined fail-safe procedures] when [Assignment: organization-defined failure conditions occur].

Supplemental Guidance

Failure conditions include, for example, loss of communications among critical system components or between system components and operational facilities. Fail-safe procedures include, for example, alerting operator personnel and providing specific instructions on subsequent steps to take (e.g., do nothing, reestablish system settings, shut down processes, restart the system, or contact designated organizational personnel).

System And Services Acquisition Control Family

Number	Control	Pivotal Application Service (PAS) Compliance
SA-1	SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES	Deployer responsibility
SA-2	ALLOCATION OF RESOURCES	Deployer responsibility
SA-3	SYSTEM DEVELOPMENT LIFE CYCLE	Deployer responsibility
SA-4	ACQUISITION PROCESS	Deployer responsibility
SA-5	INFORMATION SYSTEM DOCUMENTATION	Compliant
SA-6	SOFTWARE USAGE RESTRICTIONS	Not applicable
SA-7	USER-INSTALLED SOFTWARE	Not applicable
SA-8	SECURITY ENGINEERING PRINCIPLES	Deployer responsibility
SA-9	EXTERNAL INFORMATION SYSTEM SERVICES	Deployer responsibility
SA-10	DEVELOPER CONFIGURATION MANAGEMENT	Compliant, and deployer responsibility
SA-11	DEVELOPER SECURITY TESTING AND EVALUATION	Compliant, and deployer responsibility
SA-12	SUPPLY CHAIN PROTECTION	Not applicable
SA-13	TRUSTWORTHINESS	Not applicable
SA-14	CRITICALITY ANALYSIS	Not applicable
SA-15	DEVELOPMENT PROCESS, STANDARDS, AND TOOLS	Not applicable
SA-16	DEVELOPER-PROVIDED TRAINING	Not applicable
SA-17	DEVELOPER SECURITY ARCHITECTURE AND DESIGN	Not applicable
SA-18	TAMPER RESISTANCE AND DETECTION	
SA-19	COMPONENT AUTHENTICITY	Not applicable
SA-20	CUSTOMIZED DEVELOPMENT OF CRITICAL COMPONENTS	Not applicable
SA-21	DEVELOPER SCREENING	Not applicable
SA-22	UNSUPPORTED SYSTEM COMPONENTS	Not applicable

SA-1 SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES

PCF Compliance

All xx-1 requirements are the responsibility of the deployer. The PCF product feature set is sufficient to satisfy the technical requirements implied in SA-1. Pivotal may be able to provide guidance to customers who are creating or updating documentation, but this documentation is unique to the deployer's mission and business goals.

Control Description

The organization:

- a. 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
- b. Reviews and updates the current:
 1. System and services acquisition policy [Assignment: organization-defined frequency]; and
 2. System and services acquisition procedures [Assignment: organization-defined frequency].

Supplemental Guidance

This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the SA family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

SA-2 ALLOCATION OF RESOURCES

PCF Compliance

Compliance with the requirements defined in this control is a deployer responsibility.

Control Description

The organization:

- a. Determines information security requirements for the information system or information system service in mission/business process planning;
- b. 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
- c. Establishes a discrete line item for information security in organizational programming and budgeting documentation.

Supplemental Guidance

Resource allocation for information security includes funding for the initial information system or information system service acquisition and funding for the sustainment of the system/service.

SA-3 SYSTEM DEVELOPMENT LIFE CYCLE

PCF Compliance

Compliance with the requirements defined in this control is a deployer responsibility.

As described in these pages, the Pivotal PAS and the PCF platform will provide many of the required technical controls which previously may have been the responsibility of an individual application development team. By providing these controls as part of the deployment platform, the PCF deployment enables organizations to inherit their baseline technical controls, leaving fewer technical controls that need to be provided by the application(s).

Control Description

The organization:

- a. Manages the information system using [Assignment: organization-defined system development life cycle] that incorporates information security considerations;
- b. Defines and documents information security roles and responsibilities throughout the system development life cycle;
- c. Identifies individuals having information security roles and responsibilities; and
- d. Integrates the organizational information security risk management process into system development life cycle activities.

Supplemental Guidance

A well-defined system development life cycle provides the foundation for the successful development, implementation, and operation of organizational information systems. To apply the required security controls within the system development life cycle requires a basic understanding of information security, threats, vulnerabilities, adverse impacts, and risk to critical missions/business functions. The security engineering principles in SA-8 cannot be properly applied if individuals that design, code, and test information systems and system components (including information technology products) do not understand security. Therefore, organizations include qualified personnel, for example, chief information security officers, security architects, security engineers, and information system security officers in system development life cycle activities to ensure that security requirements are incorporated into organizational information systems. It is equally important that developers include individuals on the development team that possess the requisite security expertise and skills to ensure that needed security capabilities are effectively integrated into the information system. Security awareness and training programs can help ensure that individuals having key security roles and responsibilities have the appropriate experience, skills, and expertise to conduct assigned system development life cycle activities. The effective integration of security requirements into enterprise architecture also helps to ensure that important security considerations are addressed early in the system development life cycle and that those considerations are directly related to the organizational mission/business processes. This process also facilitates the integration of the information security architecture into the enterprise architecture, consistent with organizational risk management and information security strategies.

SA-4 ACQUISITION PROCESS

PCF Compliance

Compliance with the documentation requirements defined in this control is a deployer responsibility.

Pivotal provides [reference architecture](#) documentation for all supported IaaS environments.

These reference architecture artifacts describe the deployment environment in which a PCF deployment is intended to operate. Pivotal also provides [product security](#) documentation which will help the organization to satisfy its security-related documentation requirements.

The PCF operator delegates Identity Management functions to the existing enterprise Identity Management system, via UAA.

The deployer is responsible for integrating any approved PIV into the enterprise IdM.

Control Description

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:

- a. Security functional requirements;
- b. Security strength requirements;
- c. Security assurance requirements;
- d. Security-related documentation requirements;
- e. Requirements for protecting security-related documentation;
- f. Description of the information system development environment and environment in which the system is intended to operate; and
- g. Acceptance criteria.

Supplemental Guidance

Information system components are discrete, identifiable information technology assets (e.g., hardware, software, or firmware) that represent the building blocks of an information system. Information system components include commercial information technology products. Security functional requirements include security capabilities, security functions, and security mechanisms. Security strength requirements associated with such capabilities, functions, and mechanisms include degree of correctness, completeness, resistance to direct attack, and resistance to tampering or bypass. Security assurance requirements include: (i) development processes, procedures, practices, and methodologies; and (ii) evidence from development and assessment activities providing grounds for confidence that the required security functionality has been implemented and the required security strength has been achieved. Security documentation requirements address all phases of the system development life cycle. Security functionality, assurance, and documentation requirements are expressed in terms of security controls and control enhancements that have been selected through the tailoring process. The security control tailoring process includes, for example, the specification of parameter values through the use of assignment and selection statements and the specification of platform dependencies and implementation information. Security documentation provides user and administrator guidance regarding the implementation and operation of security controls. The level of detail required in security documentation is based on the security category or classification level of the information system and the degree to which organizations depend on the stated security capability, functions, or mechanisms to meet overall risk response expectations (as defined in the organizational risk management strategy). Security requirements can also include organizationally mandated configuration settings specifying allowed functions, ports, protocols, and services. Acceptance criteria for information systems, information system components, and information system services are defined in the same manner as such criteria for any organizational acquisition or procurement. The Federal Acquisition Regulation (FAR) Section 7.103 contains information security requirements from FISMA.

SA-5 INFORMATION SYSTEM DOCUMENTATION

PCF Compliance

Pivotal provides product documentation describing both the administrative and end-user security features of PCF. The organizational requirements included in this control may be satisfied via reference to available Pivotal [product security](#) documentation.

Control Description

The organization:

- a. 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;
- b. 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;
- c. Documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and takes [Assignment: organization-defined actions] in response;
- d. Protects documentation as required, in accordance with the risk management strategy; and
- e. Distributes documentation to [Assignment: organization-defined personnel or roles].

Supplemental Guidance

This control helps organizational personnel understand the implementation and operation of security controls associated with information systems, system components, and information system services. Organizations consider establishing specific measures to determine the quality/completeness of the content provided. The inability to obtain needed documentation may occur, for example, due to the age of the information system/component or lack of support from developers and contractors. In those situations, organizations may need to recreate selected documentation if such documentation is essential to the effective implementation or operation of security controls. The level of protection provided for selected information system, component, or service documentation is commensurate with the security category or classification of the system. For example, documentation associated with a key DoD weapons system or command and control system would typically require a higher level of protection than a routine administrative system. Documentation that addresses information system vulnerabilities may also require an increased level of protection. Secure operation of the information system, includes, for example, initially starting the system and resuming secure system operation after any lapse in system operation.

SA-6 SOFTWARE USAGE RESTRICTIONS

PCF Compliance

Not applicable.

Control Description

[Withdrawn: Incorporated into CM-10 and SI-7].

Supplemental Guidance

SA-7 USER-INSTALLED SOFTWARE

PCF Compliance

Not applicable.

Control Description

[Withdrawn: Incorporated into CM-11 and SI-7].

Supplemental Guidance

SA-8 SECURITY ENGINEERING PRINCIPLES

PCF Compliance

Compliance with the requirements defined in this control is a deployer responsibility.

Pivotal provides product documentation, including a [security guide](#) and a [reference architecture](#) document for each IaaS, that will be useful for deployers fulfilling this organizational requirement.

Control Description

The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.

Supplemental Guidance

Organizations apply security engineering principles primarily to new development information systems or systems undergoing major upgrades. For legacy systems, organizations apply security engineering principles to system upgrades and modifications to the extent feasible, given the current state of hardware, software, and firmware within those systems. Security engineering principles include, for example: (i) developing layered protections; (ii) establishing sound security policy, architecture, and controls as the foundation for design; (iii) incorporating security requirements into the system development life cycle; (iv) delineating physical and logical security boundaries; (v) ensuring that system developers are trained on how to build secure software; (vi) tailoring security controls to meet organizational and operational needs; (vii) performing threat modeling to identify use cases, threat agents, attack vectors, and attack patterns as well as compensating controls and design patterns needed to mitigate risk; and (viii) reducing risk to acceptable levels, thus enabling informed risk management decisions.

SA-9 EXTERNAL INFORMATION SYSTEM SERVICES

PCF Compliance

This requirement applies to the organization's use of third party information service providers (e.g. the IaaS or SaaS provider). Because PCF is an enterprise software product, these requirements may be considered out of scope for PCF itself.

However, all of the implied requirements are satisfiable when a PCF deployment has been implemented in accordance with the recommended reference architecture.

Control Description

The organization:

- a. Requires that providers of external information system services comply with organizational information security requirements and employ [Assignment: organization-defined security controls] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
- b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and
- c. Employs [Assignment: organization-defined processes, methods, and techniques] to monitor security control compliance by external service providers on an ongoing basis.

Supplemental Guidance

External information system services are services that are implemented outside of the authorization boundaries of organizational information systems. This includes services that are used by, but not a part of, organizational information systems. FISMA and OMB policy require that organizations using external service providers that are processing, storing, or transmitting federal information or operating information systems on behalf of the federal government ensure that such providers meet the same security requirements that federal agencies are required to meet. Organizations establish relationships with external service providers in a variety of ways including, for example, through joint ventures, business partnerships, contracts, interagency agreements, lines of business arrangements, licensing agreements, and supply chain exchanges. The responsibility for managing risks from the use of external information system services remains with authorizing officials. For services external to organizations, a chain of trust requires that organizations establish and retain a level of confidence that each participating provider in the potentially complex consumer-provider relationship provides adequate protection for the services rendered. The extent and nature of this chain of trust varies based on the relationships between organizations and the external providers. Organizations document the basis for trust relationships so the relationships can be monitored over time. External information system services documentation includes government, service providers, end user security roles and responsibilities, and service-level agreements. Service-level agreements define expectations of performance for security controls, describe measurable outcomes, and identify remedies and response requirements for identified instances of noncompliance.

SA-10 DEVELOPER CONFIGURATION MANAGEMENT

PCF Compliance

Pivotal develops PCF using a modern, agile software development process. The development processes followed for Cloud Foundry are supported by issue-tracking tools such as GitHub repositories and GitHub issues, and Pivotal Tracker. All changes made to the software are traceable via the corresponding git commit logs, and Pivotal tracker story activities. Pivotal Tracker provides workflow support that enables a team to track a work item from inception, through development, delivery, and acceptance.

Repeatable build and deployment processes may be achieved using tools such as GitHub and Concourse pipelines. Pivotal Cloud Foundry is based upon the open source software distribution of Cloud Foundry, and includes additional proprietary (closed-source) components and services. Product documentation is provided for both the OSS and commercial components. All software releases are accompanied by release notes that describe new features, included bug fixes, CVEs, and known issues.

At runtime, the BOSH director database and the Ops Manager tooling provide the configuration management capability for the PCF deployment.

Configuration management of the deployed application code is the responsibility of the application developer, but similar solution patterns may be applied.

Control Description

The organization requires the developer of the information system, system component, or information system service to:

- a. Perform configuration management during system, component, or service [Selection (one or more): design; development; implementation; operation];
- b. Document, manage, and control the integrity of changes to [Assignment: organization-defined configuration items under configuration management];
- c. Implement only organization-approved changes to the system, component, or service;
- d. Document approved changes to the system, component, or service and the potential security impacts of such changes; and
- e. Track security flaws and flaw resolution within the system, component, or service and report findings to [Assignment: organization-defined personnel].

Supplemental Guidance

This control also applies to organizations conducting internal information systems development and integration. Organizations consider the quality and completeness of the configuration management activities conducted by developers as evidence of applying effective security safeguards. Safeguards include, for example, protecting from unauthorized modification or destruction, the master copies of all material used to generate security-relevant portions of the system hardware, software, and firmware. Maintaining the integrity of changes to the information system, information system component, or information system service requires configuration control throughout the system development life cycle to track authorized changes and prevent unauthorized changes. Configuration items that are placed under configuration management (if existence/use is required by other security controls) include: the formal model; the functional, high-level, and low-level design specifications; other design data; implementation documentation; source code and hardware schematics; the running version of the object code; tools for comparing new versions of security-relevant hardware descriptions and software/firmware source code with previous versions; and test fixtures and documentation. Depending on the mission/business needs of organizations and the nature of the contractual relationships in place, developers may provide configuration management support during the operations and maintenance phases of the life cycle.

SA-11 DEVELOPER SECURITY TESTING AND EVALUATION

PCF Compliance

Compliance with the requirements defined in this control is a deployer responsibility.

A comprehensive system security assessment plan must include the people, process, and technology.

Within the technology stack, the system security assessment must include in scope the application, as well as the supporting platform, and the infrastructure.

Pivotal Cloud Foundry complies with the requirements defined in this control.

Pivotal performs comprehensive product testing on all Pivotal Cloud Foundry releases, including unit tests, integration tests, system tests, and regression tests. Pivotal issues regular releases to remediate any security vulnerabilities (CVEs) found in Cloud Foundry, and documents the history of all CVE announcements on the corresponding [security page](#) of the Pivotal Web site.

When deploying an application on Cloud Foundry, the application developers may inherit the technical and procedural controls provided by PCF, but are responsible for any controls implemented within the application itself, as well as the overall compliance of the full deployment.

Control Description

The organization requires the developer of the information system, system component, or information system service to:

- a. Create and implement a security assessment plan;
- b. Perform [Selection (one or more): unit; integration; system; regression] testing/evaluation at [Assignment: organization-defined depth and coverage];
- c. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation;
- d. Implement a verifiable flaw remediation process; and
- e. Correct flaws identified during security testing/evaluation.

Supplemental Guidance

Developmental security testing/evaluation occurs at all post-design phases of the system development life cycle. Such testing/evaluation confirms that the required security controls are implemented correctly, operating as intended, enforcing the desired security policy, and meeting established security requirements. Security properties of information systems may be affected by the interconnection of system components or changes to those components. These interconnections or changes (e.g., upgrading or replacing applications and operating systems) may adversely affect previously implemented security controls. This control provides additional types of security testing/evaluation that developers can conduct to reduce or eliminate potential flaws. Testing custom software applications may require approaches such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Developers can employ these analysis approaches in a variety of tools (e.g., web-based application scanners, static analysis tools, binary analyzers) and in source code reviews. Security assessment plans provide the specific activities that developers plan to carry out including the types of analyses, testing, evaluation, and reviews of software and firmware components, the degree of rigor to be applied, and the types of artifacts produced during those processes. The depth of security testing/evaluation refers to the rigor and level of detail associated with the assessment process (e.g., black box, gray box, or white box testing). The coverage of security testing/evaluation refers to the scope (i.e., number and type) of the artifacts included in the assessment process. Contracts specify the acceptance criteria for security assessment plans, flaw remediation processes, and the evidence that the plans/processes have been diligently applied. Methods for reviewing and protecting assessment plans, evidence, and documentation are commensurate with the security category or classification level of the information system. Contracts may specify documentation protection requirements.

SA-12 SUPPLY CHAIN PROTECTION

PCF Compliance

This control is not required at the FISMA moderate level.

Pivotal develops PCF using open source software, and an agile development methodology which includes pair programming for continuous code review. In addition, Pivotal provides regular security updates for PCF. Deployers with unique supply chain protection requirements may contact the Pivotal Security Team at security@pivotal.io.

Control Description

The organization protects against supply chain threats to the information system, system component, or information system service by employing [Assignment: organization-defined security safeguards] as part of a comprehensive, defense-in-breadth information security strategy.

Supplemental Guidance

Information systems (including system components that compose those systems) need to be protected throughout the system development life cycle (i.e., during design, development, manufacturing, packaging, assembly, distribution, system integration, operations, maintenance, and retirement). Protection of organizational information systems is accomplished through threat awareness, by the identification, management, and reduction of vulnerabilities at each phase of the life cycle and the use of complementary, mutually reinforcing strategies to respond to risk. Organizations consider implementing a standardized process to address supply chain risk with respect to information systems and system components, and to educate the acquisition workforce on threats, risk, and required security controls. Organizations use the acquisition/procurement processes to require supply chain entities to implement necessary security safeguards to: (i) reduce the likelihood of unauthorized modifications at each stage in the supply chain; and (ii) protect information systems and information system components, prior to taking delivery of such systems/components. This control also applies to information system services. Security safeguards include, for example: (i) security controls for development systems, development facilities, and external connections to development systems; (ii) vetting development personnel; and (iii) use of tamper-evident packaging during shipping/warehousing. Methods for reviewing and protecting development plans, evidence, and documentation are commensurate with the security category or classification level of the information system. Contracts may specify documentation protection requirements.

SA-13 TRUSTWORTHINESS

PCF Compliance

Not applicable.

Control Description

The organization:

- a. Describes the trustworthiness required in the [Assignment: organization-defined information system, information system component, or information system service] supporting its critical missions/business functions; and
- b. Implements [Assignment: organization-defined assurance overlay] to achieve such trustworthiness.

Supplemental Guidance

This control helps organizations to make explicit trustworthiness decisions when designing, developing, and implementing information systems that are needed to conduct critical organizational missions/business functions. Trustworthiness is a characteristic/property of an information system that expresses the degree to which the system can be expected to preserve the confidentiality, integrity, and availability of the information it processes, stores, or transmits. Trustworthy information systems are systems that are capable of being trusted to operate within defined levels of risk despite the environmental disruptions, human errors, and purposeful attacks that are expected to occur in the specified environments of operation. Trustworthy systems are important to mission/business success. Two factors affecting the trustworthiness of information systems include: (i) security functionality (i.e., the security features, functions, and/or mechanisms employed within the system and its environment of operation); and (ii) security assurance (i.e., the grounds for confidence that the security functionality is effective in its application). Developers, implementers, operators, and maintainers of organizational information systems can increase the level of assurance (and trustworthiness), for example, by employing well-defined security policy models, structured and rigorous hardware, software, and firmware development techniques, sound system/security engineering principles, and secure configuration settings (defined by a set of assurance-related security controls in Appendix E). Assurance is also based on the assessment of evidence produced during the system development life cycle. Critical missions/business functions are supported by high-impact systems and the associated assurance requirements for such systems. The additional assurance controls in Table E-4 in Appendix E (designated as optional) can be used to develop and implement high-assurance solutions for specific information systems and system components using the concept of overlays described in Appendix I. Organizations select assurance overlays that have been developed, validated, and approved for community adoption (e.g., cross-organization, governmentwide), limiting the development of such overlays on an organization-by-organization basis. Organizations can conduct criticality analyses as described in SA-14, to determine the information systems, system components, or information system services that require high-assurance solutions. Trustworthiness requirements and assurance overlays can be described in the security plans for organizational information systems.

SA-14 CRITICALITY ANALYSIS

PCF Compliance

Not applicable.

Control Description

The organization identifies critical information system components and functions by performing a criticality analysis for [Assignment: organization-defined information systems, information system components, or information system services] at [Assignment: organization-defined decision points in the system development life cycle].

Supplemental Guidance

Criticality analysis is a key tenet of supply chain risk management and informs the prioritization of supply chain protection activities such as attack surface reduction, use of all-source intelligence, and tailored acquisition strategies. Information system engineers can conduct an end-to-end functional decomposition of an information system to identify mission-critical functions and components. The functional decomposition includes the identification of core organizational missions supported by the system, decomposition into the specific functions to perform those missions, and traceability to the hardware, software, and firmware components that implement those functions, including when the functions are shared by many components within and beyond the information system boundary. Information system components that allow for unmediated access to critical components or functions are considered critical due to the inherent vulnerabilities such components create. Criticality is assessed in terms of the impact of the function or component failure on the ability of the component to complete the organizational missions supported by the information system. A criticality analysis is performed whenever an architecture or design is being developed or modified, including upgrades.

SA-15 DEVELOPMENT PROCESS, STANDARDS, AND TOOLS

PCF Compliance

Not applicable.

Control Description

The organization:

- a. Requires the developer of the information system, system component, or information system service to follow a documented development process that:
 - 1. Explicitly addresses security requirements;
 - 2. Identifies the standards and tools used in the development process;
 - 3. Documents the specific tool options and tool configurations used in the development process; and
 - 4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and
- b. Reviews the development process, standards, tools, and tool options/configurations [Assignment: organization-defined frequency] to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy [Assignment: organization-defined security requirements].

Supplemental Guidance

Development tools include, for example, programming languages and computer-aided design (CAD) systems. Reviews of development processes can include, for example, the use of maturity models to determine the potential effectiveness of such processes. Maintaining the integrity of changes to tools and processes enables accurate supply chain risk assessment and mitigation, and requires robust configuration control throughout the life cycle (including design, development, transport, delivery, integration, and maintenance) to track authorized changes and prevent unauthorized changes.

SA-16 DEVELOPER-PROVIDED TRAINING

PCF Compliance

Not applicable.

Control Description

The organization requires the developer of the information system, system component, or information system service to provide [Assignment: organization-defined training] on the correct use and operation of the implemented security functions, controls, and/or mechanisms.

Supplemental Guidance

This control applies to external and internal (in-house) developers. Training of personnel is an essential element to ensure the effectiveness of security controls implemented within organizational information systems. Training options include, for example, classroom-style training, web-based/computer-based training, and hands-on training. Organizations can also request sufficient training materials from developers to conduct in-house training or offer self-training to organizational personnel. Organizations determine the type of training necessary and may require different types of training for different security functions, controls, or mechanisms.

SA-17 DEVELOPER SECURITY ARCHITECTURE AND DESIGN

PCF Compliance

Not applicable.

Control Description

The organization requires the developer of the information system, system component, or information system service to produce a design specification and security architecture that:

- a. Is consistent with and supportive of the organization's security architecture which is established within and is an integrated part of the organization's enterprise architecture;
- b. Accurately and completely describes the required security functionality, and the allocation of security controls among physical and logical components; and
- c. Expresses how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection.

Supplemental Guidance

This control is primarily directed at external developers, although it could also be used for internal (in-house) development. In contrast, PL-8 is primarily directed at internal developers to help ensure that organizations develop an information security architecture and such security architecture is integrated or tightly coupled to the enterprise architecture. This distinction is important if/when organizations outsource the development of information systems, information system components, or information system services to external entities, and there is a requirement to demonstrate consistency with the organization's enterprise architecture and information security architecture.

SA-18 TAMPER RESISTANCE AND DETECTION

PCF Compliance

Not applicable.

Control Description

The organization implements a tamper protection program for the information system, system component, or information system service.

Supplemental Guidance

Anti-tamper technologies and techniques provide a level of protection for critical information systems, system components, and information technology products against a number of related threats including modification, reverse engineering, and substitution. Strong identification combined with tamper resistance and/or tamper detection is essential to protecting information systems, components, and products during distribution and when in use.

SA-19 COMPONENT AUTHENTICITY

PCF Compliance

Not applicable.

Control Description

The organization:

- a. Develops and implements anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the information system; and
- b. Reports counterfeit information system components to [Selection (one or more): source of counterfeit component; [Assignment: organization-defined external reporting organizations]; [Assignment: organization-defined personnel or roles]].

Supplemental Guidance

Sources of counterfeit components include, for example, manufacturers, developers, vendors, and contractors. Anti-counterfeiting policy and procedures support tamper resistance and provide a level of protection against the introduction of malicious code. External reporting organizations include, for example, US-CERT.

SA-20 CUSTOMIZED DEVELOPMENT OF CRITICAL COMPONENTS

PCF Compliance

Not applicable.

Control Description

The organization re-implements or custom develops [Assignment: organization-defined critical information system components].

Supplemental Guidance

Organizations determine that certain information system components likely cannot be trusted due to specific threats to and vulnerabilities in those components, and for which there are no viable security controls to adequately mitigate the resulting risk. Re-implementation or custom development of such components helps to satisfy requirements for higher assurance. This is accomplished by initiating changes to system components (including hardware, software, and firmware) such that the standard attacks by adversaries are less likely to succeed. In situations where no alternative sourcing is available and organizations choose not to re-implement or custom develop critical information system components, additional safeguards can be employed (e.g., enhanced auditing, restrictions on source code and system utility access, and protection from deletion of system and application files).

SA-21 DEVELOPER SCREENING

PCF Compliance

Not applicable.

Control Description

The organization requires that the developer of [Assignment: organization-defined information system, system component, or information system service]:

- a. Have appropriate access authorizations as determined by assigned [Assignment: organization-defined official government duties]; and
- b. Satisfy [Assignment: organization-defined additional personnel screening criteria].

Supplemental Guidance

Because the information system, system component, or information system service may be employed in critical activities essential to the national and/or economic security interests of the United States, organizations have a strong interest in ensuring that the developer is trustworthy. The degree of trust required of the developer may need to be consistent with that of the individuals accessing the information system/component/service once deployed. Examples of authorization and personnel screening criteria include clearance, satisfactory background checks, citizenship, and nationality. Trustworthiness of developers may also include a review and analysis of company ownership and any relationships the company has with entities potentially affecting the quality/reliability of the systems, components, or services being developed.

SA-22 UNSUPPORTED SYSTEM COMPONENTS

PCF Compliance

Not applicable.

Control Description

The organization:

- a. Replaces information system components when support for the components is no longer available from the developer, vendor, or manufacturer;
and
- b. Provides justification and documents approval for the continued use of unsupported system components required to satisfy mission/business needs.

Supplemental Guidance

Support for information system components includes, for example, software patches, firmware updates, replacement parts, and maintenance contracts. Unsupported components (e.g., when vendors are no longer providing critical software patches), provide a substantial opportunity for adversaries to exploit new weaknesses discovered in the currently installed components. Exceptions to replacing unsupported system components may include, for example, systems that provide critical mission/business capability where newer technologies are not available or where the systems are so isolated that installing replacement components is not an option.