Centers for Medicare & Medicaid Services

Catalog of Minimum Acceptable Risk Controls for Exchanges – Exchange Reference Architecture Supplement

Version 1.0

August 1, 2012

Foreword

The *Exchange Reference Architecture: Foundation Guidance*, Version 1.0, provides the business, information, and technical architecture approach and technical standards for the health insurance Exchanges. The Foundation Guidance document provides an overview and description of the approaches to defining the architectures; the Centers for Medicare & Medicaid Services (CMS) will release additional Exchange Reference Architecture (ERA) supplements to provide engineering detail allowing Exchange implementation and operations personnel to build systems and environments that adhere to the approved Exchange Architecture as well as other Exchange information technology (IT) standards, data safeguards, and requirements.

CMS's Deputy Chief Information Officer (DCIO) leads the development of this Architecture with the support of the Exchanges and all components of the IT staff and contractors. The ERA consists of the Foundation Guidance document and the CMS ERA Supplements, authorized and approved by the CMS DCIO. CMS has reviewed and accepted this Architecture Framework as a foundational component of CMS's Enterprise Architecture in accordance with the CMS IT governance process.

In accordance with the agency's Information Security program, CMS has developed this *Catalog of Minimum Acceptable Risk Controls for Exchanges – Exchange Reference Architecture Supplement* to establish the specific controls for data. Two companion documents, the *Harmonized Security and Privacy Framework – Exchange Reference Supplement*, and *Minimum Acceptable Risk Standards for Exchanges – Exchange Reference Architecture Supplement,* define a risk-based Security and Privacy Framework for use in the design and implementation of Exchange IT systems for which CMS has oversight responsibility. Together, these documents, along with the four documents in the ACA System Security Plan Document Suite,[1] form Version 1.0 of the *Minimum Acceptable Risk Standards for Exchanges* Document Suite (also known as the "MARS-E Suite").

The guidance contained in these documents also applies to other Affordable Care Act Administering Entities. "Administering Entity" means a state Medicaid Agency, state Children's Health Insurance Program (CHIP), a state basic health program (BHP), or an Exchange.

As noted in the *Minimum Acceptable Risk Standards for Exchanges,* this Catalog presents those minimum security controls essential to execution of its guidance. CMS has reviewed and accepted this *Catalog of Minimum Acceptable Risk Controls for Exchanges* as a component of the Exchange Reference Architecture in accordance with the CMS IT governance process.

CMS has circulated this document for review by the following signatory federal partner agencies that share data with the Exchanges through the CMS Data Services Hub. Each agency concurs with the MARS-E Suite guidance, as demonstrated by signature ("/s/") of the authorized signatories for each federal partner agency.

Any changes to this *Catalog of Minimum Acceptable Risk Controls for Exchanges – Exchange Reference Architecture Supplement* must be approved by the CMS DCIO, the CMS Chief Information Security Officer, and the CMS Chief Technology Officer.

[1] The suite consists of the *ACA System Security Plan Procedures*, Version 1.0; *ACA System Security Plan Template*, Version 1.0; *ACA System Security Plan*, Workbook; and *ACA Internal Revenue Service Safeguard Procedures Report Template*.

/s/

Tony Trenkle Date
Chief Information Officer
Centers for Medicare & Medicaid Services

/s/

Henry Chao Date
Deputy Chief Information Officer
Centers for Medicare & Medicaid Services

/s/

Mark Hogle Date
Chief Technology Officer
Centers for Medicare & Medicaid Services

/s/

Teresa Fryer Date
Chief Information Security Officer
Office of Information Services
Centers for Medicare & Medicaid Services

Federal Partner Agency Concurrence and Approval

The following federal partner agency signatories have reviewed and concur with the guidance contained in the following documents known as the MARS-E Document Suite:

- *Harmonized Security and Privacy Framework – Exchange Reference Architecture Supplement*, Version 1.0
- *Minimum Acceptable Risk Standards for Exchanges – Exchange Reference Architecture Supplement*, Version 1.0
- *Catalog of Minimum Acceptable Risk Controls for Exchanges – Exchange Reference Architecture Supplement*, Version 1.0
- *ACA System Security Plan Procedures*, Version 1.0
- *ACA System Security Plan Template*, Version 1.0
- *ACA System Security Plan Workbook,* Version 1.0
- *ACA Internal Revenue Service Safeguard Procedures Report Template,* Version 1.0

SEEN AND APPROVED:

Internal Revenue Service

Terence V. Milholland Chief Technology Officer	/s/ Signature	Date
S. Gina Garza ACIO, Affordable Care Act (PMO)	/s/ Signature	Date

Social Security Administration

Kelly Croft Deputy Commissioner for Systems and Chief Information Officer	/s/ Signature	Date
Brad Flick Associate Commissioner and Chief Information Security	/s/ Signature	Date

Department of Veterans Affairs

Jerry Davis Deputy Assistant Secretary and Chief Information Security Officer	/s/ Signature	Date
John Oswalt Associate Deputy Assistant Secretary for Policy, Privacy and Incident Response	/s/ Signature	Date

Department of Homeland Security

Mark Schwartz ____________________/s/______________ ______________
USCIS Chief Information Officer Signature Date

Perry Darley ____________________/s/______________ ______________
USCIS Chief Information Security Signature Date
Officer

Department of Defense

Dr. Karen Guice ____________________/s/______________ ______________
Chief Information Officer Signature Date

COL Lorraine Breen ____________________/s/______________ ______________
Acting Chief Information Officer Signature Date

Peace Corps

Dorine Andrews ____________________/s/______________ ______________
Chief Information Officer Signature Date

Falan Memmott ____________________/s/______________ ______________
Director of IT Security Assurance Signature Date
& Compliance

Office of Personnel Management

Matthew Perry ____________________/s/______________ ______________
Chief Information Officer Signature Date

Andy Newton ____________________/s/______________ ______________
Chief Information Security Officer Signature Date

Record of Changes

Version Number	Date	Author/Owner	Description of Change	CR #
1.0	August 1, 2012	CMS	Final version 1.0 for publication	N/A

CR: Change Request

Table of Contents

List of Tables

Introduction

The Patient Protection and Affordable Care Act of 2010[2] (hereafter simply the "Affordable Care Act") provides for each state to have a health insurance Exchange. An Exchange is an organized marketplace to help consumers and small businesses to buy health insurance in a way that permits easy comparison of available plan options based on price, benefits and services, and quality. Consumers seeking health care coverage will be able to go to the health insurance Exchanges to obtain comprehensive information on coverage options currently available and make informed health insurance choices. By pooling consumers, reducing transaction costs, and increasing transparency, Exchanges create more efficient and competitive health insurance markets for individuals and small businesses.

Section 1561 of the Affordable Care Act requires the Department of Health and Human Services (HHS), in consultation with the Health Information Technology (HIT) Policy Committee and the HIT Standards Committee (the Committees), to develop interoperable and secure standards and protocols that facilitate electronic enrollment of individuals in federal and state health and human services programs.

The Department of Health and Human Services (HHS) and the Centers for Medicare & Medicaid Services (CMS) are responsible for providing guidance and oversight for the Exchanges and for state IT systems that facilitate common electronic enrollment. This responsibility includes defining business, information, and technical guidance that will create a common baseline and standards for these IT system implementation activities. CMS will focus this guidance on the key tradeoffs and technology choices necessary to create interoperable and coordinated IT services between the federal government and the Exchanges.

1.1 *Purpose*

Protecting and ensuring the confidentiality, integrity, and availability for Exchange information systems is the responsibility of the Exchanges; the Affordable Care Act charges CMS with responsibility for oversight of the Exchange and common enrollment IT systems. This *Catalog of Minimum Security Controls for Exchanges – Exchange Reference Architecture Supplement* (hereafter simply "MARS-E") defines a set of security controls that focuses on the most common vulnerabilities hackers use to exploit systems.

The purpose of this supplement is to augment the security guidance for use by the Exchanges in implementing and operating their IT systems in support of the Affordable Care Act. Each Exchange system owner is responsible for incorporating the security controls defined in this document with other state-appropriate security and privacy requirements, and for documenting the control implementation details in the Exchange's System Security Plan (SSP). Exchanges also are required to define system risks in an Information Security (IS) Risk Assessment (RA).

Depending on the information processed, an Exchange's IT system may be required to meet additional security control requirements as mandated by specific federal, state, legal, program, or accounting sources. For example, an Exchange may be a "covered entity" under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH). When Exchanges handle Protected Health Information (PHI), they are subject to these laws. In addition, when the

[2] Public Law 111-148, Patient Protection and Affordable Care Act, March 23, 2010, 124 Stat. 119, http://www.gpo.gov/fdsys/pkg/PLAW-111publ148/content-detail.html
http://www.healthreform.gov/health_reform_and_hhs.html

Exchanges carry out business functions that require data sources provided by federal or state entities, each of the data sharing instances carries obligations for protecting the security and privacy of the shared data based on owner specifications. For instance, Internal Revenue Code (IRC) 26 U.S.C. §6103 applies if an Exchange IT system receives Federal Tax Information (FTI). Therefore, Exchanges must develop their IT systems to comply with these standards when applicable. The guidance in this supplement neither relieves nor waives any other federal, state, or other applicable laws, guidance, policies, or standards.

1.2 *Scope*

This document identifies the set of Minimum Security Controls for state IT systems for which CMS has oversight responsibility, starting with Exchanges and common program enrollment systems as required by the Affordable Care Act. The Minimum Security Controls identified in this supplement assume that the applicable state IT system is classified as Moderate and contains Personally Identifiable Information (PII).

1.3 *Taxonomy of this Catalog*

CMS has organized the catalog to present CMS's prescribed Minimum Security Controls into 19 control families within three classes (management, operational, and technical) to provide ease of use. CMS adopted the families in accordance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*.

Each family contains security controls related to the security functionality of the family. A two-character identifier is assigned to uniquely identify each of the security control families. Some of the controls within a family may have characteristics that can be in more than one class. The class predominantly supported by the family is the class designation for the entire family. Table 1 summarizes the security control families and the two-character identifier used in this catalog.

Table 1. Family Descriptions for Minimum Security Controls for Exchanges

Family (and Identifier)	Class	Description
Access Control (AC)	Technical	The standards listed in this section focus on how the Exchange shall limit IT system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems), and to the types of transactions and functions that authorized users are permitted to exercise.
Awareness and Training (AT)	Operational	The standards listed in this section focus on how the Exchange shall: (i) ensure that managers and users of Exchange IT systems are made aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of IT systems; and (ii) ensure that Exchange personnel are adequately trained to carry out their assigned IS-related duties and responsibilities.

Family (and Identifier)	Class	Description
Audit and Accountability (AU)	Technical	The standards listed in this section focus on how the Exchange shall: (i) create, protect, and retain IT system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate IT system activity; and (ii) ensure that the actions of individual IT system users can be uniquely traced to those users so they can be held accountable for their actions.
Security Assessment and Authorization (CA)	Management	The standards listed in this section focus on how the Exchange shall: (i) periodically assess the security controls in Exchange IT systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in Exchange IT systems; (iii) authorize the operation of Exchange IT systems and any associated IT system connections; and (iv) monitor IT system security controls on an ongoing basis to ensure the continued effectiveness of the controls.
Configuration Management (CM)	Operational	The standards listed in this section focus on how the Exchange shall: (i) establish and maintain baseline configurations and inventories of Exchange IT systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for IT technology products employed in Exchange IT systems.
Contingency Planning (CP)	Operational	The standards listed in this section focus on how the Exchange shall establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for Exchange IT systems to ensure the availability of critical information resources and continuity of operations in emergency situations.
Identification and Authentication (IA)	Technical	The standards listed in this section focus on how the Exchange shall identify IT system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to Exchange IT systems.
Incident Response (IR)	Operational	The standards listed in this section focus on how the Exchange shall: (i) establish an operational incident handling capability for Exchange IT systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate Exchange officials and/or authorities.
Maintenance (MA)	Operational	The standards listed in this section focus on how the Exchange shall: (i) perform periodic and timely maintenance on organizational information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.
Media Protection (MP)	Operational	The standards listed in this section focus on how the Exchange shall: (i) protect IT system media, both paper and digital; (ii) limit access to information on IT system media to authorized users; and (iii) sanitize or destroy IT system media before disposal or release for reuse.

Family (and Identifier)	Class	Description
Physical and Environmental Protection (PE)	Operational	The standards listed in this section focus on how the Exchange shall: (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.
Planning (PL)	Management	The standards listed in this section focus on how the Exchange shall develop, document, periodically update, and implement security plans for Exchange IT systems that describe the security controls in place or planned for the IT systems and the rules of behavior for individuals accessing the IT systems.
Personnel Security (PS)	Operational	The standards listed in this section focus on how the Exchange shall: (i) ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with organizational security policies and procedures.
Risk Assessment (RA)	Management	The standards listed in this section focus on how the Exchange shall periodically assess the risk to Exchange operations (including mission, functions, image, or reputation), Exchange assets, and individuals, resulting from the operation of Exchange IT systems and the associated processing, storage, or transmission of Exchange information.
System and Services Acquisition (SA)	Management	The standards listed in this section focus on how the Exchange shall: (i) allocate sufficient resources to adequately protect Exchange IT systems; (ii) employ system development life cycle processes that incorporate IS considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.
System and Communications Protection (SC)	Technical	The standards listed in this section focus on how the Exchange shall: (i) monitor, control, and protect Exchange communications (i.e., information transmitted or received by Exchange IT systems) at the external boundaries and key internal boundaries of the IT systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective IS within Exchange IT systems.
System and Information Integrity (SI)	Operational	The standards listed in this section focus on how the Exchange shall: (i) identify, report, and correct information and IT system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within Exchange IT systems; and (iii) monitor IT system security alerts and advisories, and take appropriate actions in response.

Family (and Identifier)	Class	Description
Program Management (PM)	Management	The standards listed in this section complement the security controls in the above 17 families by focusing on the organization-wide information security requirements that are essential for managing information security programs.
FTI Safeguards		The standards listed in this section are additional controls required by IRS Publication 1075

1.4 *Intended Audience*

The Catalog of Minimum Acceptable Risk Controls for Exchanges – Exchange Reference Architecture Supplement provides details on the Minimum Acceptable Risk Controls for Exchanges for use in the design, implementation, operation, and maintenance of the Exchange IT systems for which CMS has oversight responsibility, and has received the explicit approval of the CMS Deputy Chief Information Officer (DCIO), CMS Chief Information Security Officer, and CMS Chief Technology Officer. CMS has authorized distribution of this document to all Exchanges, other federal agencies, CMS staff, CMS Production Environment contractors, The MITRE Corporation [the Agency's Federally Funded Research and Development Center (FFRDC) advisor], and any entity given explicit access to this document through CMS executive or management approval.

1.5 *Relationship to Other Documents*

The *Catalog of Minimum Acceptable Risk Controls for Exchanges – Exchange Reference Architecture Supplement* must be read in conjunction with the companion *Minimum Acceptable Risk Standards for Exchanges – Exchange Reference Architecture Supplement* and the List of References presented in that document.

1.6 *Document Organization*

The following 19 sections present the descriptions of the specific minimum security controls by Family and Class.

Access Control (AC) – Technical

Table 2. AC-1: Access Control Policy and Procedures

<table>
<tr><th colspan="3">AC-1: Access Control Policy and Procedures</th></tr>
<tr><td colspan="3"><b>Control</b></td></tr>
<tr><td colspan="3">The organization develops, disseminates, and reviews/updates within every three-hundred-sixty-five (365) days:
a. A formal, documented access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
b. Formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.</td></tr>
<tr><td colspan="3"><b>Guidance</b></td></tr>
<tr><td colspan="3">This control is intended to produce the policy and procedures that are required for the effective implementation of Exchange security controls and control enhancements in the access control family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The access control policy can be included as part of the general information security policy for the organization. Access control procedures can be developed for the security program in general and for a particular Exchange information system, when required. The organizational risk management strategy is a key factor in the development of the access control policy.</td></tr>
<tr><td><b>Applicability:</b> Exchanges</td><td><b>Reference(s):</b> HIPAA: 164.308(a)(3)(ii)(A), 164.308(a)(4)(ii)(C); IRS-1075: 9.2</td><td><b>Related Control Requirements:</b></td></tr>
<tr><td colspan="3"><b>Assessment Procedure: AC-1.1</b></td></tr>
<tr><td colspan="3"><b>Assessment Objective</b></td></tr>
<tr><td colspan="3">Determine if:</td></tr>
<tr><td colspan="3">(i) the organization develops and formally documents access control policy;
(ii) the organization access control policy addresses:
– purpose;
– scope;
– roles and responsibilities;
– management commitment;
– coordination among organizational entities;
– compliance;
(iii) the organization disseminates formal documented access control policy to elements within the organization having associated access control roles and responsibilities;
(iv) the organization develops and formally documents access control procedures;
(v) the organization access control procedures facilitate implementation of the access control policy and associated access controls;
(vi) the organization disseminates formal documented access control procedures to elements within the organization having associated access control roles and responsibilities;
(vii) the organization reviews/updates the access control policy and procedures within every three-hundred-sixty-five (365) days.</td></tr>
<tr><td colspan="3"><b>Assessment Methods and Objects</b></td></tr>
<tr><td colspan="3"><b>Examine:</b> Access control policy and procedures; other relevant documents or records.</td></tr>
<tr><td colspan="3"><b>Interview:</b> Organizational personnel with access control responsibilities.</td></tr>
</table>

Table 3. AC-2: Account Management

AC-2: Account Management

Control

The organization manages Exchange information system accounts, including:

a. Identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary);
b. Establishing conditions for group membership;
c. Identifying authorized users of the information system and specifying access privileges;
d. Requiring appropriate approvals for requests to establish accounts;
e. Establishing, activating, modifying, disabling, and removing accounts;
f. Specifically authorizing and monitoring the use of guest/anonymous and temporary accounts;
g Notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes;
h. Deactivating: (i) temporary accounts that are no longer required; and (ii) accounts of terminated or transferred users;
i. Granting access to the system based on: (i) a valid access authorization; (ii) intended system usage; and (iii) other attributes as required by the organization or associated missions/business functions; and
j. Reviewing accounts using the frequency specified in Implementation Standard 1.

For FTI: The agency must ensure that only authorized employees or contractors (as allowed by statute) of the agency receiving the information have access to FTI.

Implementation Standards

1. Review information system accounts within every one-hundred-eighty (180) days and require annual certification.
2. Remove or disable default user accounts. Rename active default accounts.
3. Implement centralized control of user access administrator functions.
4. Regulate the access provided to contractors and define security requirements for contractors.

Guidance

The identification of authorized users of the Exchange information system and the specification of access privileges is consistent with the requirements in other security controls in the security plan. Users requiring administrative privileges on information system accounts receive additional scrutiny by organizational officials responsible for approving such accounts and privileged access.

Applicability: Exchanges	**Reference(s):** HIPAA: 164.308(a)(3)(ii)(B), 164.308(a)(4)(i), 164.308(a)(4)(ii)(B); IRS-1075: 9.2	**Related Control Requirements:**

Assessment Procedure: AC-2.1

Assessment Objective

Determine if:

(i) the organization manages information system accounts, including;
- identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary);
- establishing conditions for group membership;
- identifying authorized users of the information system and specifying access privileges;
- requiring appropriate approvals for requests to establish accounts;
- establishing, activating, modifying, disabling, and removing accounts;
- specifically authorizing and monitoring the use of guest/anonymous and temporary accounts;
- notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes;
- deactivating: (a) temporary accounts that are no longer required; and (b) accounts of terminated or transferred users;
- granting access to the system based on: (a) a valid access authorization; (b) intended system usage; and (c) other attributes as required by the organization or associated missions/business functions;

AC-2: Account Management
(ii) the organization reviews information system accounts in accordance with the frequency specified in Implementation Standard 1. (iii) the organization meets all the requirements specified in the applicable implementation standard(s).
Assessment Methods and Objects
Examine: Access control policy; procedures addressing account management; security plan; list of active system accounts along with the name of the individual associated with each account; list of guest/anonymous and temporary accounts along with the name of the individual associated with the each account and the date the account expires; lists of recently transferred, separated, or terminated employees; list of recently disabled information system accounts along with the name of the individual associated with each account; system-generated records with user IDs and last login date; other relevant documents or records.
Interview: Organizational personnel with account management responsibilities.

Table 4. AC-2(2): Configuration of Emergency Account

AC-2(2): Configuration of Emergency Account		
Control		
The information system automatically terminates emergency accounts within twenty-four (24) hours and temporary accounts with a fixed duration not to exceed three-hundred sixty-five (365) days.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.2	**Related Control Requirements:**
Assessment Procedure: AC-2(2).1		
Assessment Objective		
Determine if:		
(i) the organization defines in the System Security Plan, explicitly or by reference, a time period for each type of account after which the information system terminates temporary and emergency accounts; (ii) the information system automatically terminates temporary and emergency accounts after organization-defined time period for each type of account.		
Assessment Methods and Objects		
Examine: Security plan; information system design documentation; information system configuration settings and associated documentation; information system-generated list of active accounts; information system audit records; other relevant documents or records.		

Table 5. AC-2(3): Disable Inactive Accounts

AC-2(3): Disable Inactive Accounts		
Control		
The information system automatically disables inactive accounts after one-hundred-eighty (180) days.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.2	**Related Control Requirements:**
Assessment Procedure: AC-2(3).1		
Assessment Objective		
Determine if:		
(i) the organization defines in the System Security Plan, explicitly or by reference, a time period after which the information system disables inactive accounts; (ii) the information system automatically disables inactive accounts after organization-defined time period.		
Assessment Methods and Objects		

AC-2(3): Disable Inactive Accounts
Examine: Procedures addressing account management; security plan; information system design documentation; information system configuration settings and associated documentation; information system-generated list of last login dates; information system-generated list of active accounts; information system audit records; other relevant documents or records.

Table 6. AC-2(4): Automatic Audit and Notification

AC-2(4): Automatic Audit and Notification		
Control		
The information system automatically audits account creation, modification, disabling, and termination actions and notifies, as required, appropriate individuals.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.2	**Related Control Requirements:**
Assessment Procedure: AC-2(4).1		
Assessment Objective		
Determine if:		

(i) the information system automatically audits:
– account creation;
– modification;
– disabling;
– termination actions;
(ii) the information system notifies, as required, appropriate individuals.		

Assessment Methods and Objects		
Examine: Procedures addressing account management; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.		

Table 7. AC-3: Access Enforcement

AC-3: Access Enforcement
Control
The information system enforces approved authorizations for logical access to the system in accordance with applicable policy.
Implementation Standards
1. If encryption is used as an access control mechanism, it must meet approved (FIPS 140-2 compliant and a NIST-validated module) encryption standards (see SC-13). 2. Configure operating system controls to disable public "read" and "write" access to files, objects, and directories that may directly impact system functionality and/or performance, or that contain sensitive information (such as FTI or Privacy Act protected information). 3. Data stored in the information system must be protected with system access controls.
Guidance
Access control policies (e.g., identity-based policies, role-based policies, attribute-based policies) and access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) are employed by organizations to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system. In addition to enforcing authorized access at the information-system level, access enforcement mechanisms are employed at the application level, when necessary, to provide increased information security for the organization. Consideration is given to the implementation of an audited, explicit override of automated mechanisms in the event of emergencies or other serious events. If encryption of stored information is employed as an access enforcement mechanism, the cryptography used is FIPS 140-2 (as amended) compliant.

AC-3: Access Enforcement		
Encryption as access enforcement extends to all government and non-government furnished desktop computers that store sensitive information. While encryption is the preferred technical solution for protection of sensitive information on all desktop computers, adequate physical security controls and other management controls are acceptable mitigations for the protection of desktop computers with the approval of the CIO or his/her designated representative. Mechanisms implemented by AC-3 are configured to enforce authorizations determined by other security controls.		
Applicability: Exchanges	**Reference(s):** HIPAA: 164.310(a)(2)(iii), 164.312(a)(1); IRS-1075: 9.2	**Related Control Requirements:** SC-13
Assessment Procedure: AC-3.1		
Assessment Objective		
Determine if:		
(i) the information system enforces approved authorizations for logical access to the system in accordance with applicable policy. (ii) the organization meets all the requirements specified in the applicable implementation standard(s).		
Assessment Methods and Objects		
Examine: Access control policy; procedures addressing access enforcement; information system configuration settings and associated documentation; list of approved authorizations (user privileges); information system audit records; other relevant documents or records.		

Table 8. AC-4: Information Flow Enforcement

AC-4: Information Flow Enforcement		
Control		
The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.		
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. A few examples of flow control restrictions include: keeping export controlled information from being transmitted in the clear to the Internet, blocking outside traffic that claims to be from within the organization, and not passing any web requests to the Internet that are not from the internal web proxy. Information flow control policies and enforcement mechanisms are commonly employed by organizations to control the flow of information between designated sources and destinations (e.g., networks, individuals, devices) within information systems and between interconnected systems. Flow control is based on the characteristics of the information and/or the information path. Specific examples of flow control enforcement can be found in boundary protection devices (e.g., proxies, gateways, guards, encrypted tunnels, firewalls, and routers) 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 content (e.g., using key word searches or document characteristics). Mechanisms implemented by AC-4 are configured to enforce authorizations determined by other security controls.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.2	**Related Control Requirements:** SC-7
Assessment Procedure: AC-4.1		
Assessment Objective		
Determine if:		
(i) the organization defines applicable policy for controlling the flow of information within the system and between interconnected systems; (ii) the organization defines approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy; (iii) the information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.		
Assessment Methods and Objects		

AC-4: Information Flow Enforcement
Examine: Access control policy; procedures addressing information flow enforcement; information system design documentation; information system configuration settings and associated documentation; information system baseline configuration; list of information flow authorizations; information system audit records; other relevant documents or records.

Table 9. AC-5: Separation of Duties

<table>
<tr><th colspan="3">AC-5: Separation of Duties</th></tr>
<tr><td colspan="3"><b>Control</b></td></tr>
<tr><td colspan="3">The organization:
a. Separates duties of individuals as necessary, to prevent malevolent activity without collusion;
b. Documents separation of duties; and
c. Implements separation of duties through assigned information system access authorizations.</td></tr>
<tr><td colspan="3"><b>Implementation Standards</b></td></tr>
<tr><td colspan="3">1. Ensure that audit functions are not performed by security personnel responsible for administering access control.
2. Maintain a limited group of administrators with access based upon the users' roles and responsibilities.
3. Ensure that critical mission functions and information system support functions are divided among separate individuals.
4. Ensure that information system testing functions (i.e., user acceptance, quality assurance, information security) and production functions are divided among separate individuals or groups.
5. Ensure that an independent entity, not the Business Owner, System Developer(s)/Maintainer(s), or System Administrator(s) responsible for the information system, conducts information security testing of the information system.</td></tr>
<tr><td colspan="3"><b>Guidance</b></td></tr>
<tr><td colspan="3">Examples of separation of duties include: (i) mission functions and distinct information system support functions are divided among different individuals/roles; (ii) different individuals perform information system support functions (e.g., system management, systems programming, configuration management, quality assurance and testing, network security); (iii) security personnel who administer access control functions do not administer audit functions; and (iv) different administrator accounts for different roles. Access authorizations defined in this control are implemented by control AC-3.</td></tr>
<tr><td><b>Applicability:</b> Exchanges</td><td><b>Reference(s):</b> IRS-1075: 9.2</td><td><b>Related Control Requirements:</b> AC-3.</td></tr>
<tr><td colspan="3"><b>Assessment Procedure: AC-5.1</b></td></tr>
<tr><td colspan="3"><b>Assessment Objective</b></td></tr>
<tr><td colspan="3">Determine if:</td></tr>
<tr><td colspan="3">(i) the organization separates duties of individuals as necessary, to prevent malevolent activity without collusion;
(ii) the organization documents separation of duties; and
(iii) the organization implements separation of duties through assigned information system access authorizations.</td></tr>
<tr><td colspan="3"><b>Assessment Methods and Objects</b></td></tr>
<tr><td colspan="3"><b>Examine:</b> Access control policy; procedures addressing divisions of responsibility and separation of duties; information system configuration settings and associated documentation; list of divisions of responsibility and separation of duties; information system audit records; other relevant documents or records.</td></tr>
<tr><td colspan="3"><b>Interview:</b> Organizational personnel with responsibilities for defining appropriate divisions of responsibility and separation of duties.</td></tr>
</table>

Table 10. AC-6: Least Privilege

AC-6: Least Privilege		
Control		
The organization: a. Employs the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) that are necessary to accomplish assigned tasks in accordance with Exchange missions and business functions. For FTI: Access to FTI must be strictly on a need-to-know basis. FTI must never be indiscriminately disseminated, even within the recipient agency, body, or commission. No person should be given more FTI than is needed for performance of his/her duties.		
Implementation Standards		
1. Disable all file system access not explicitly required for system, application, and administrator functionality. 2. Contractors must be provided with minimal system and physical access, and must agree to and support the security requirements. The contractor selection process must assess the contractor's ability to adhere to and support security policy. 3. Restrict the use of database management utilities to only authorized database administrators. Prevent users from accessing database data files at the logical data view, field, or field-value level. Implement table-level access control. 4. Ensure that only authorized users are permitted to access those files, directories, drives, workstations, servers, network shares, ports, protocols, and services that are expressly required for the performance of job duties. 5. Disable all system and removable media boot access unless it is explicitly authorized by the organizational CIO for compelling operational needs. If authorized, boot access is password protected.		
Guidance		
The access authorizations defined in this control are largely implemented by control AC-3. The organization employs the concept of least privilege for specific duties (including specific ports, protocols, and services) in accordance with risk assessments as necessary to adequately mitigate risk to operations and assets, individuals, other organizations, and the Nation.		
Applicability: Exchanges	**Reference(s):** HIPAA: 164.308(a)(3)(i), 164.308(a)(4)(ii)(A); IRS-1075: 9.2	**Related Control Requirements:** AC-3
Assessment Procedure: AC6.1		
Assessment Objective		
Determine if:		
(i) the organization employs the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. (ii) the organization meets all the requirements specified in the applicable implementation standard(s).		
Assessment Methods and Objects		
Examine: Access control policy; procedures addressing least privilege; list of assigned access authorizations (user privileges); information system configuration settings and associated documentation; information system audit records; other relevant documents or records.		
Interview: Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks.		

Table 11. AC-6(2): Use of Non-Privileged Accounts

AC-6(2): Use of Non-Privileged Accounts
Control
The organization requires that users of information system accounts, or roles, with access to administrator accounts or security functions, use non-privileged accounts, or roles, when accessing other system functions, and if feasible, audits any use of privileged accounts, or roles, for such functions.

AC-6(2): Use of Non-Privileged Accounts		
Guidance		
This control enhancement is intended to limit exposure due to operating from within a privileged account or role. The inclusion of role is intended to address those situations where an access control policy such as Role-Based Access Control (RBAC) is being implemented and where a change of role provides the same degree of assurance in the change of access authorizations for both the user and all processes acting on behalf of the user as would be provided by a change between a privileged and non-privileged account. Audit of privileged activity may require physical separation employing information systems on which the user does not have privileged access.		
Applicability: Exchanges	**Reference(s):**	**Related Control Requirements:**
Assessment Procedure: AC-6(2).1		
Assessment Objective		
Determine if:		
(i) the organization defines the security functions or security-relevant information to which users of information system accounts, or roles, have access; (ii) the organization requires that users of information system accounts, or roles, with access to organization-defined security functions or security-relevant information, use non-privileged accounts, or roles, when accessing other system functions; (iii) the organization, if deemed feasible, audits any use of privileged accounts, or roles, with access to organization-defined security functions or security-relevant information, when accessing other system functions.		
Assessment Methods and Objects		
Examine: Access control policy; procedures addressing least privilege; list of system-generated security functions or security-relevant information assigned to information system accounts or roles; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.		
Interview: Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks.		

Table 12. AC-7: Unsuccessful Login Attempts

AC-7: Unsuccessful Login Attempts		
Control		
The information system: a. Enforces the limit of consecutive invalid login attempts by a user specified in Implementation Standard 1 during the time period specified in Implementation Standard 1; and b. Automatically disables or locks the account/node until released after the time period specified in Implementation Standard 1 when the maximum number of unsuccessful attempts is exceeded. The control applies regardless of whether the login occurs via a local or network connection.		
Implementation Standards		
1. Configure the information system to lock out the user account automatically after three (3) failed log-on attempts by a user. For FTI: Automatically lock the account/node until an authorized system administrator reinstates the account.		
Guidance		
Due to the potential for denial of service, automatic lockouts initiated by the information system are usually temporary and automatically release after a predetermined time period established by the organization. If a delay algorithm is selected, the organization may chose to employ different algorithms for different information system components based on the capabilities of those components. Response to unsuccessful login attempts may be implemented at both the operating system and the application levels. This control applies to all accesses other than those accesses explicitly identified and documented by the organization in AC-14.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.2	**Related Control Requirements:**

AC-7: Unsuccessful Login Attempts

Assessment Procedure: AC-7.1

Assessment Objective

Determine if:

(i) the organization defines the maximum number of consecutive invalid login attempts to the information system by a user and the time period in which the consecutive invalid attempts occur;

(ii) the information system enforces the organization-defined limit of consecutive invalid login attempts by a user during the organization-defined time period;

(iii) the organization defines action to be taken by the system when the maximum number of unsuccessful login attempts is exceeded as:

- lock out the account/node for a specified time period;
- lock out the account/note until released by an administrator; or
- delay the next login prompt according to organization-defined delay algorithm;

(iv) the information system either automatically locks the account/node for the organization-defined time period, locks the account/node until released by an administrator, or delays next login prompt for the organization-defined delay period when the maximum number of unsuccessful login attempts is exceeded; and

(v) the information system performs the organization-defined actions when the maximum number of unsuccessful login attempts is exceeded regardless of whether the login occurs via a local or network connection.

Assessment Methods and Objects

Examine: Access control policy; procedures addressing unsuccessful login attempts; security plan; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

Table 13. AC-8: System Use Notification

AC-8: System Use Notification

Control

The information system:

a. Displays an approved 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. The approved banner for information systems is:

– You are accessing a U.S. Government information system, which includes: (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only.

– Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties.

– By using this information system, you understand and consent to the following:

* You have no reasonable expectation of privacy regarding any communication or data transiting or stored on this information system. At any time, and for any lawful Government purpose, the Government may monitor, intercept, and search and seize any communication or data transiting or stored on this information system.

* Any communication or data transiting or stored on this information system may be disclosed or used for any lawful Government purpose.

b. Retains the notification message or banner on the screen until users take explicit actions to log on to or further access the information system; and

c. For publicly accessible systems: (i) displays the system use information when appropriate, before granting further access; (ii) displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and (iii) includes in the notice given to public users of the information system, a description of the authorized uses of the system.

For FTI: The warning banner must contain reference to the civil and criminal penalty sections of Title 26 Sections 7213, 7213A and 7431.

Guidance

System use notification messages can be implemented in the form of warning banners displayed when individuals log in to the information system. System use notification is intended only for information system access that includes an interactive login interface with a human user and is not intended to require notification when an interactive interface does not exist.

Applicability: Exchanges	**Reference(s):** IRS-1075: 9.2	**Related Control Requirements:**

Assessment Procedure: AC-8.1

Assessment Objective

Determine if:

(i) the organization approves the information system use notification message or banner to be displayed by the information system before granting access to the system;

(ii) the information system displays the approved 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:

– users are accessing a U.S. Government information system;

– system usage may be monitored, recorded, and subject to audit;

– unauthorized use of the system is prohibited and subject to criminal and civil penalties; and

– use of the system indicates consent to monitoring and recording; and

(iii) the information system retains the notification message or banner on the screen until the user takes explicit actions to log on to or further access the information system.

AC-8: System Use Notification
Assessment Methods and Objects
Examine: Access control policy; privacy and security policies; procedures addressing system use notification; documented approval of information system use notification messages or banners; information system notification messages; information system configuration settings and associated documentation; information system audit records for user acceptance of notification message or banner; other relevant documents or records.
Assessment Procedure: AC-8.2
Assessment Objective
Determine if:
(i) the information system (for publicly accessible systems) displays the system use information when appropriate, before granting further access; (ii) the information system (for publicly accessible systems) displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and (iii) the information system (for publicly accessible systems) includes in the notice given to public users of the information system, a description of the authorized uses of the information system.
Assessment Methods and Objects
Examine: Access control policy; privacy and security policies; procedures addressing system use notification; documented approval of information system use notification messages or banners; information system notification messages; information system configuration settings and associated documentation; other relevant documents or records.

Table 14. AC-10: Concurrent Session Control

<table>
<tr><th colspan="3">AC-10: Concurrent Session Control</th></tr>
<tr><td colspan="3"><b>Control</b></td></tr>
<tr><td colspan="3">The information system limits the number of concurrent sessions for each system account to one (1) session. The number of concurrent application/process sessions is limited and enforced to the number of sessions expressly required for the performance of job duties and any requirement for more than one (1) concurrent application/process session is documented in the security plan.</td></tr>
<tr><td colspan="3"><b>Guidance</b></td></tr>
<tr><td colspan="3">The organization may define the maximum number of concurrent sessions for an information system account globally, by account type, by account, or a combination. This control addresses concurrent sessions for a given information system account and does not address concurrent sessions by a single user via multiple system accounts.</td></tr>
<tr><td><b>Applicability:</b> Exchanges</td><td><b>Reference(s):</b></td><td><b>Related Control Requirements:</b></td></tr>
<tr><td colspan="3"><b>Assessment Procedure: AC-10.1</b></td></tr>
<tr><td colspan="3"><b>Assessment Objective</b></td></tr>
<tr><td colspan="3">Determine if:</td></tr>
<tr><td colspan="3">(i) the organization defines the maximum number of concurrent sessions to be allowed for each system account; and
(ii) the information system limits the number of concurrent sessions for each system account to the organization-defined number of sessions.</td></tr>
<tr><td colspan="3"><b>Assessment Methods and Objects</b></td></tr>
<tr><td colspan="3"><b>Examine:</b> Access control policy; procedures addressing concurrent session control; information system design documentation; information system configuration settings and associated documentation; security plan; other relevant documents or records.</td></tr>
</table>

Table 15. AC-11: Session Lock

AC-11: Session Lock		
Control		
The information system: a. Prevents further access to the system by initiating a session lock after fifteen (15) minutes of inactivity; and c. Retains the session lock until the user reestablishes access using established identification and authentication procedures.		
Guidance		
A session lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not want to log out because of the temporary nature of the absence. The session lock is implemented at the point where session activity can be determined. This is typically at the operating system-level, but may be at the application-level. A session lock is not a substitute for logging out of the information system, for example, if the organization requires users to log out at the end of the workday.		
Applicability: Exchanges	**Reference(s):**	**Related Control Requirements:**
Assessment Procedure: AC-11.1		
Assessment Objective		
Determine if:		
(i) the organization defines the time period of user inactivity after which the information system initiates a session lock; (ii) the information system initiates a session lock after the organization-defined time period of inactivity or upon receiving a request from a user; (iii) the information system retains the session lock until the user reestablishes access using established identification and authentication procedures.		
Assessment Methods and Objects		
Examine: Access control policy; procedures addressing session lock; information system design documentation; information system configuration settings and associated documentation; security plan; other relevant documents or records.		

Table 16. AC-14: Permitted Actions without Identification or Authentication

AC-14: Permitted Actions without Identification or Authentication
Control
The organization: a. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification and authentication; and b. Configures Information systems to permit public access only to the extent necessary to accomplish mission objectives, without first requiring individual identification and authentication.
Implementation Standard
1. Identify and document specific user actions that can be performed on the information system without identification or authentication.
Guidance
This control is intended for those specific instances where an organization determines that no identification and authentication is required; it is not, however, mandating that such instances exist in given information system. The organization may allow a limited number of user actions without identification and authentication (e.g., when individuals access public websites or other publicly accessible federal information systems such as http://www.usa.gov). Organizations also identify any actions that normally require identification or authentication but may under certain circumstances (e.g., emergencies), allow identification or authentication mechanisms to be bypassed. Such bypass may be, for example, via a software-readable physical switch that commands bypass of the login 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 being repeated, but rather to situations where identification and/or authentication have not yet occurred.

AC-14: Permitted Actions without Identification or Authentication		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.2	**Related Control Requirements:** CP-2, IA-2
Assessment Procedure: AC-14.1		
Assessment Objective		
Determine if:		
(i) the organization identifies specific user actions that can be performed on the information system without identification or authentication; and (ii) the organization documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification and authentication.		
Assessment Methods and Objects		
Examine: Access control policy; procedures addressing permitted actions without identification and authentication; information system configuration settings and associated documentation; security plan; list of information system actions that can be performed without identification and authentication; information system audit records; other relevant documents or records.		

Table 17. AC-14(1): Permitted Action without Identification or Authentication

AC-14(1): Permitted Action without Identification or Authentication		
Control		
The organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission/business objectives.		
Guidance		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.2	**Related Control Requirements:**
Assessment Procedure: AC-14(1).1		
Assessment Objective		
Determine if the organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission/business objectives.		
Assessment Methods and Objects		
Examine: Access control policy; procedures addressing permitted actions without identification and authentication; information system configuration settings and associated documentation; security plan; list of information system actions that can be performed without identification and authentication; information system audit records; other relevant documents or records.		

Table 18. AC-17: Remote Access

AC-17: Remote Access
Control
Remote access for privileged functions shall be permitted only for compelling operational needs, shall be strictly controlled, and must be explicitly authorized, in writing, by the CIO or his/her designated representative. If authorized, the organization: a. Documents allowed methods of remote access to the information system; b. Establishes usage restrictions and implementation guidance for each allowed remote access method; c. Monitors for unauthorized remote access to the information system; d. Authorizes remote access to the information system prior to connection; and e. Enforces requirements for remote connections to the information system. For FTI: For remote access to FTI, encrypted modems and/or Virtual Private Networks (VPN) are required for every workstation and a smart card (microprocessor) for every user. Smart cards must have both identification and

AC-17: Remote Access

authentication features and must provide data encryption as well. Two-factor authentication is required whenever FTI is being accessed from an alternate work location or if accessing FTI via the agency's web portal.

Implementation Standards

1. Require callback capability with re-authentication to verify connections from authorized locations when the secure data communications network or Multi-Protocol Label Switching (MPLS) service network cannot be used.
2. If e-authentication is implemented as a remote access solution or associated with remote access, refer to NIST SP 800-63, *Electronic Authentication Guideline*.

Guidance

This control requires explicit authorization prior to allowing remote access to an information system without specifying a specific format for that authorization. For example, while the organization may deem it appropriate to use a system interconnection agreement to authorize a given remote access, such agreements are not required by this control. Remote access is any access to an information system by a user (or process acting on behalf of a user) communicating through an external network (e.g., the Internet). Examples of remote access methods include dial-up, broadband, and wireless (see AC-18 for wireless access). A virtual private network (VPN) when adequately provisioned with appropriate security controls, is considered an internal network (i.e., the organization establishes a network connection between organization-controlled endpoints in a manner that does not require the organization to depend on external networks to protect the confidentiality or integrity of information transmitted across the network). Remote access controls are applicable to information systems other than public web servers or systems specifically designed for public access. Enforcing access restrictions associated with remote connections is accomplished by control AC-3.

Applicability: Exchanges	**Reference(s):** IRS-1075: 9.18.3	**Related Control Requirements:** IA-2, SC-9

Assessment Procedure: AC-17.1

Assessment Objective

Determine if:

(i) the organization documents allowed methods of remote access to the information system;
(ii) the organization establishes usage restrictions and implementation guidance for each allowed remote access method;
(iii) the organization monitors for unauthorized remote access to the information system;
(iv) the organization authorizes remote access to the information system prior to connection;
(v) the organization enforces requirements for remote connections to the information system.
(vi) the organization meets all the requirements specified in the applicable implementation standard(s).

Assessment Methods and Objects

Examine: Access control policy; procedures addressing remote access to the information system; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

Interview: Organizational personnel with remote access authorization, monitoring, and control responsibilities

Table 19. AC-17(1): Automated Remote Access Monitoring

AC-17(1): Automated Remote Access Monitoring

Control

The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods.

Guidance

Automated monitoring of remote access sessions allows organizations to audit user activities on a variety of information system components (e.g., servers, workstations, notebook/laptop computers) and to ensure compliance with remote access policy.

Applicability: Exchanges	**Reference(s):** IRS-1075: 9.18.3	**Related Control Requirements:**

AC-17(1): Automated Remote Access Monitoring
Assessment Procedure: AC-17(1).1
Assessment Objective
Determine if the information system employs automated mechanisms to facilitate the monitoring and control of remote access methods.
Assessment Methods and Objects
Examine: Access control policy; procedures addressing remote access to the information system; information system configuration settings and associated documentation; other relevant documents or records.

Table 20. AC-17(3): Managed Access Control Points Use

AC-17(3): Managed Access Control Points Use		
Control		
The information system routes all remote accesses through a limited number of managed access control points.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.2	**Related Control Requirements:**
Assessment Procedure: AC-17(3).1		
Assessment Objective		
Determine if:		
(i) the organization defines a limited number of managed access control points for remote access to the information system; (ii) the information system routes all remote accesses through managed access control points.		
Assessment Methods and Objects		
Examine: Access control policy; procedures addressing remote access to the information system; information system design documentation; list of managed access control points; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.		

Table 21. AC-18: Wireless Access

AC-18: Wireless Access
Control
The organization prohibits the installation of wireless access points (WAP) to Exchange information systems unless explicitly authorized, in writing, by the CIO or his/her designated representative. If authorized, the organization: a. Monitors for unauthorized wireless access to the information system; and b. Enforces requirements for wireless connections to the information system.
Implementation Standards
1. If wireless access is explicitly approved, wireless device service set identifier broadcasting is disabled and the following wireless access controls are implemented: a. Encryption protection is enabled; b. Access points are placed in secure areas; c. Access points are shut down when not in use (i.e., nights, weekends); d. A firewall is implemented between the wireless network and the wired infrastructure; e, MAC address authentication is utilized; f. Static IP addresses, not DHCP, is utilized; g. Personal firewalls are utilized on all wireless clients; h. File sharing is disabled on all wireless clients; i. Intrusion detection agents are deployed on the wireless side of the firewall; and j. Wireless activity is monitored and recorded, and the records are reviewed on a regular basis.

AC-18: Wireless Access		
Guidance		
Wireless technologies include, but are not limited to, microwave, satellite, 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. In certain situations, wireless signals may radiate beyond the confines and control of organization-controlled facilities.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.2	**Related Control Requirements:**
Assessment Procedure: AC-18.1		
Assessment Objective		
Determine if:		
(i) the organization establishes usage restrictions and implementation guidance for wireless access; (ii) the organization monitors for unauthorized wireless access to the information system; (iii) the organization authorizes wireless access to the information system prior to connection; (iv) the organization enforces requirements for wireless connections to the information system. (v) the organization meets all the requirements specified in the applicable implementation standard(s).		
Assessment Methods and Objects		
Examine: Access control policy; procedures addressing wireless implementation and usage (including restrictions); activities related to wireless monitoring, authorization, and enforcement; information system audit records; other relevant documents or records.		
Interview: Organizational personnel responsible for authorizing, monitoring or controlling the use of wireless technologies in the information system.		

Table 22. AC-18(1): Wireless Access Authentication and Encryption

AC-18(1): Wireless Access Authentication and Encryption		
Control		
If wireless access is explicitly approved, the information system protects wireless access to the system using authentication and encryption. For FTI: The agency shall authorize, document, and monitor all wireless access to the information system in accordance with NIST 800-48 Revision 1.		
Guidance		
Authentication applies to user, device, or both as necessary.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.2	**Related Control Requirements:**
Assessment Procedure: AC-18(1).1		
Assessment Objective		
Determine if the information system protects wireless access to the system using authentication and encryption.		
Assessment Methods and Objects		
Examine: Access control policy; procedures addressing wireless implementation and usage (including restrictions); information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.		

Table 23. AC-19: Access Control for Mobile Devices

AC-19: Access Control for Mobile Devices

Control

The organization prohibits the connection of portable and mobile devices [e.g., notebook computers, personal digital assistants (PDA(, cellular telephones, and other computing and communications devices with network connectivity and the capability of periodically operating in different physical locations] to Exchange information systems unless explicitly authorized, in writing, by the CIO or his/her designated representative. If authorized, the organization:

a. Employs an approved method of cryptography (see SC-13) to protect information residing on portable and mobile information devices, and utilizes whole-disk encryption solution for laptops;

b. Monitors for unauthorized connections of mobile devices to information systems;

c. Enforces requirements for the connection of mobile devices to information systems;

d. Disables information system functionality that provides the capability for automatic execution of code on mobile devices without user direction;

e. Issues specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk in accordance with organizational policies and procedures; and

f. Protects the storage and transmission of information on portable and mobile information devices with activities such as scanning the devices for malicious code, virus protection software.

Guidance

Mobile devices include portable storage media (e.g., USB memory sticks, external hard disk drives) and portable computing and communications devices with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices). Organization-controlled mobile devices include those devices for which the organization has the authority to specify and the ability to enforce specific security requirements. Usage restrictions and implementation guidance related to 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). Examples of information system functionality that provide the capability for automatic execution of code are AutoRun and AutoPlay.

Organizational policies and procedures for mobile devices used by individuals departing on and returning from travel include, for example, determining which locations are of concern, defining required configurations for the devices, ensuring that the devices are configured as intended before travel is initiated, and applying specific measures to the device after travel is completed. Specially configured mobile devices include, for example, computers with sanitized hard drives, limited applications, and additional hardening (e.g., more stringent configuration settings). Specified measures applied to mobile devices upon return from travel include, for example, examining the device for signs of physical tampering and purging/reimaging the hard disk drive. Protecting information residing on mobile devices is covered in the media protection family.

Applicability: Exchanges	**Reference(s):** IRS-1075: 9.2	**Related Control Requirements:**

Assessment Procedure: AC-19.1

Assessment Objective

Determine if:

(i) the organization prohibits the connection of portable and mobile devices to the information system unless explicitly authorized, in writing, by the CIO;

(ii) if authorized, the organization employs an approved method of cryptography (see SC-13) to protect information residing on portable and mobile information devices, and utilizes whole-disk encryption solution for laptops;

(iii) if authorized, the organization monitors for unauthorized connections of mobile devices to organizational information systems;

(iv) if authorized, the organization enforces requirements for the connection of mobile devices to organizational information systems;

(v) if authorized, the organization disables information system functionality that provides the capability for automatic execution of code on mobile devices without user direction;

(vi) if authorized, the organization issues specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk in accordance with organizational policies and

AC-19: Access Control for Mobile Devices
procedures; (vii) if authorized, the organization defines the inspection and preventative measures to be applied to mobile devices returning from locations that the organization deems to be of significant risk; (viii) if authorized, the organization applies organization-defined inspection and preventative measures to mobile devices returning from locations that the organization deems to be of significant risk in accordance with organizational policies and procedures.
Assessment Methods and Objects
Examine: Access control policy; procedures addressing access control for portable and mobile devices; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.
Interview: Organizational personnel who use portable and mobile devices to access the information system.

Table 24. AC-20: Use of External Information Systems

AC-20: Use of External Information Systems
Control
The organization prohibits the use of external information systems, including but not limited to, Internet kiosks, personal desktop computers, laptops, tablet personal computers, personal digital assistant (PDA) devices, cellular telephones, facsimile machines, and equipment available in hotels or airports to store, access, transmit, or process sensitive information (such as FTI or Privacy Act protected information), unless explicitly authorized, in writing, by the CIO or his/her designated representative. If authorized, the organization establishes strict terms and conditions for their use. The terms and conditions shall address, at a minimum: a. The types of applications that can be accessed from external information systems; b. The maximum FIPS 199 security category of information that can be processed, stored, and transmitted; c. How other users of the external information system will be prevented from accessing federal information; d. The use of virtual private networking (VPN) and firewall technologies; e. The use of and protection against the vulnerabilities of wireless technologies; f. The maintenance of adequate physical security controls; g. The use of virus and spyware protection software; and h. How often the security capabilities of installed software are to be updated.
Implementation Standards
1. Instruct all personnel working from home to implement fundamental security controls and practices, including passwords, virus protection, and personal firewalls. Limit remote access only to information resources required by home users to complete job duties. Require that any government-owned equipment be used only for business purposes by authorized employees. 2. (For PII only) Only organization owned computers and software can be used to process, access, and store PII. For FTI: 3. If the agency allows alternative work sites, such as an employee’s home or other non-traditional work sites, the FTI remains subject to the same safeguard requirements as the agency’s offices. (Pub. 1075, Ref 4.7) 4. Only agency-owned computers, media, and software will be used to receive, process, access, and store FTI. The agency must retain ownership and control for the security configuration of all hardware, software, and end-point equipment connecting to public communication networks including encryption keys. (Pub. 1075, Ref 4.7.1)
Guidance
External information systems are information systems or components of information systems that are outside of the authorization boundary established by the organization and for which the organization typically has no direct supervision and authority over the application of required security controls or the assessment of security control effectiveness. External information systems include, but are not limited to: (i) personally owned information systems (e.g., computers, cellular telephones, or personal digital assistants); (ii) privately owned computing and communications devices resident in commercial or public facilities (e.g., hotels, convention centers, or airports); (iii) information systems owned or controlled by nonfederal governmental organizations; and (iv) federal information

AC-20: Use of External Information Systems

systems that are not owned by, operated by, or under the direct supervision and authority of the organization. For some external systems, in particular those systems operated by other federal agencies, including organizations subordinate to the Exchange, 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. In effect, the information systems of these organizations would not be considered external. These situations typically occur when, for example, there is some pre-existing sharing or trust agreement (either implicit or explicit) established between federal agencies and/or organizations subordinate to those agencies, or such trust agreements are specified by applicable laws, Executive Orders, directives, or policies.

This control does not apply to the use of external information systems to access public interfaces to information systems and information (e.g., individuals accessing federal information through www.medicare.gov). The organization establishes terms and conditions for the use of external information systems in accordance with security policies and procedures. The terms and conditions address at a minimum (i) the types of applications that can be accessed on the information system from the external information system; and (ii) the maximum security categorization of information that can be processed, stored, and transmitted on the external information system. This control defines access authorizations enforced by AC-3, and session establishment rules enforced by AC-17.

Applicability: Exchanges	**Reference(s):** IRS-1075: 9.2	**Related Control Requirements:**

Assessment Procedure: AC-20.1

Assessment Objective

Determine if:

(i) the organization prohibits the use of external information systems to store, access, transmit, or process sensitive information unless explicitly authorized, in writing, by the CIO;

(ii) if authorized, the organization identifies individuals authorized to:
- access the information system from the external information systems;
- process, store, and/or transmit organization-controlled information using the external information systems;

(iii) if authorized, the terms and conditions address, at a minimum:
- the types of applications that can be accessed from external information systems;
- the maximum FIPS-199 security category of information that can be processed, stored, and transmitted;
- how other users of the external information system will be prevented from accessing federal information;
- the use of virtual private networking (VPN) and firewall technologies;
- the use of and protection against the vulnerabilities of wireless technologies;
- the maintenance of adequate physical security controls;
- the use of virus and spyware protection software; and
- how often the security capabilities of installed software are to be updated.

(iv) the organization meets all the requirements specified in the applicable implementation standard(s).

(v) only organizational owned computers and software are used to process, access, and store PII.

Assessment Methods and Objects

Examine: Access control policy; procedures addressing the use of external information systems; external information systems terms and conditions; list of types of applications accessible from external information systems; maximum security categorization for information processed, stored, or transmitted on external information systems; information system configuration settings and associated documentation; other relevant documents or records.

Interview: Organizational personnel with responsibilities for defining terms and conditions for use of external information systems to access organizational systems.

Awareness and Training (AT) – Operational

Table 25. AT-1: Security Awareness and Training Policy and Procedures

AT-1: Security Awareness and Training Policy and Procedures		
Control		
The organization develops, disseminates, and reviews/updates within every three-hundred-sixty-five (365) days: a. A formal, documented security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.		
Guidance		
This control is intended to produce the policy and procedures that are required for the effective implementation of security controls and control enhancements in the security awareness and training family. he policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The security awareness and training policy can be included as part of the general information security policy for the organization. Security awareness and training procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the security awareness and training policy.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.4	**Related Control Requirements:**
Assessment Procedure: AT-1.1		
Assessment Objective		
Determine if:		
(i) the organization develops and formally documents security awareness and training policy; (ii) the organization security awareness and training policy addresses: – purpose; – scope; – roles and responsibilities; – management commitment; – coordination among organizational entities, and compliance; (iii) the organization disseminates formal documented security awareness and training policy to elements within the organization having associated security awareness and training roles and responsibilities; (iv) the organization develops and formally documents security awareness and training procedures; (v) the organization security awareness and training procedures facilitate implementation of the security awareness and training policy and associated security awareness and training controls; (vi) the organization disseminates formal documented security awareness and training procedures to elements within the organization having associated security awareness and training roles and responsibilities; (vii) the organization reviews/updates the security awareness and training policy and procedures within every three-hundred-sixty-five (365) days.		
Assessment Methods and Objects		
Examine: Security awareness and training policy and procedures; other relevant documents or records.		
Interview: Organizational personnel with security awareness and training responsibilities.		

Table 26. AT-2: Security Awareness

<table>
<tr><th colspan="3">AT-2: Security Awareness</th></tr>
<tr><td colspan="3"><b>Control</b></td></tr>
<tr><td colspan="3">The organization provides basic security awareness training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users prior to accessing any system's information, when required by system changes, and within every three-hundred sixty-five (365) days thereafter.
For FTI: Awareness training specific to protecting FTI and the sanctions for misuse of FTI must be provided initially prior to granting access to FTI and annually thereafter.</td></tr>
<tr><td colspan="3"><b>Guidance</b></td></tr>
<tr><td colspan="3">The organization determines the appropriate content of security awareness training and security awareness techniques based on the specific requirements of the organization 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 as it relates to the information security program. 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.</td></tr>
<tr><td><b>Applicability:</b> Exchanges</td><td><b>Reference(s):</b> HIPAA: 164.308(a)(5)(i); IRS-1075: 6.2, 9.4</td><td><b>Related Control Requirements:</b></td></tr>
<tr><td colspan="3"><b>Assessment Procedure: AT-2.1</b></td></tr>
<tr><td colspan="3"><b>Assessment Objective</b></td></tr>
<tr><td colspan="3">Determine if:</td></tr>
<tr><td colspan="3">(i) the organization provides basic security awareness training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users and when required by system changes;
(ii) the organization defines in the security plan, explicitly or by reference, the frequency of refresher security awareness training and the frequency is at least annually;
(iii) the organization provides refresher security awareness training in accordance with the organization-defined frequency.</td></tr>
<tr><td colspan="3"><b>Assessment Methods and Objects</b></td></tr>
<tr><td colspan="3"><b>Examine:</b> Security awareness and training policy; procedures addressing security awareness training implementation; appropriate codes of federal regulations; security awareness training curriculum; security awareness training materials; security plan; training records; other relevant documents or records.</td></tr>
<tr><td colspan="3"><b>Interview:</b> Organizational personnel comprising the general information system user community.</td></tr>
</table>

Table 27. AT-3: Security Training

<table>
<tr><th>AT-3: Security Training</th></tr>
<tr><td><b>Control</b></td></tr>
<tr><td>The organization provides role-based security-related training: (i) before authorizing access to the system or performing assigned duties; (ii) when required by system changes; and (iii) refresher training within every three-hundred-sixty-five (365) days thereafter.
For FTI: The disclosure awareness requirements apply to all agency employees with access to FTI, including program and information technology personnel and contractors, such as case workers, managers, system administrators, database administrators and application developers.</td></tr>
<tr><td><b>Implementation Standards</b></td></tr>
<tr><td>1. Require personnel with significant information security roles and responsibilities to undergo appropriate information system security training prior to authorizing access to networks, systems, and/or applications; when required by system changes; and refresher training within every three-hundred-sixty-five (365) days thereafter.</td></tr>
</table>

<table>
<tr><th colspan="3">AT-3: Security Training</th></tr>
<tr><td colspan="3"><b>Guidance</b></td></tr>
<tr><td colspan="3">The organization determines the appropriate content of security training based on assigned roles and responsibilities and the specific requirements of the information systems to which personnel have authorized access. In addition, the organization provides information system managers, system and network administrators, personnel performing independent verification and validation activities, security control assessors, and other personnel having access to system-level software, adequate security-related technical training to perform their assigned duties. Organizational security training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical safeguards and countermeasures. The organization also provides the training necessary for these individuals to carry out their responsibilities related to operations security within the context of information security program.</td></tr>
<tr><td><b>Applicability:</b> Exchanges</td><td><b>Reference(s):</b> IRS-1075: 6.2, 9.4</td><td><b>Related Control Requirements:</b></td></tr>
<tr><td colspan="3"><b>Assessment Procedure: AT-3.1</b></td></tr>
<tr><td colspan="3"><b>Assessment Objective</b></td></tr>
<tr><td colspan="3">Determine if:</td></tr>
<tr><td colspan="3">(i) the organization provides role-based security-related training before authorizing access to the system or performing assigned duties, and when required by system changes;
(ii) the organization provides role-based security-related refresher training within every three-hundred-sixty-five (365) days thereafter;
(iii) the organization meets all the requirements specified in the applicable implementation standard(s).</td></tr>
<tr><td colspan="3"><b>Assessment Methods and Objects</b></td></tr>
<tr><td colspan="3"><b>Examine:</b> Security awareness and training policy; procedures addressing security training implementation; codes of federal regulations; security training curriculum; security training materials; security plan; training records; other relevant documents or records.</td></tr>
<tr><td colspan="3"><b>Interview:</b> Organizational personnel with responsibilities for role-based, security-related training; organizational personnel with significant information system security responsibilities.</td></tr>
</table>

Table 28. AT-4: Security Training Records

<table>
<tr><th colspan="3">AT-4: Security Training Records</th></tr>
<tr><td colspan="3"><b>Control</b></td></tr>
<tr><td colspan="3">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 three (3) years.
For FTI: Granting employees or contractors access to FTI must be preceded by each employee or contractor certifying his/her understanding of the agency’s security policy and procedures for safeguarding FTI. The certification must be maintained for 5 years.</td></tr>
<tr><td colspan="3"><b>Guidance</b></td></tr>
<tr><td colspan="3">While an organization may deem that organizationally mandated individual training programs and the development of individual training plans are necessary, this control does not mandate either. Documentation for specialized training may be maintained by individual supervisors at the option of the organization.</td></tr>
<tr><td><b>Applicability:</b> Exchanges</td><td><b>Reference(s):</b> IRS-1075: 6.2, 9.4</td><td><b>Related Control Requirements:</b></td></tr>
<tr><td colspan="3"><b>Assessment Procedure: AT-4.1</b></td></tr>
</table>

AT-4: Security Training Records
Assessment Objective
Determine if:
(i) the organization documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; (ii) the organization defines the time period for retaining individual training records; and (iii) the organization retains individual training records in accordance with the organization-defined time period.
Assessment Methods and Objects
Examine: Security awareness and training policy; procedures addressing security training records; security awareness and training records; other relevant documents or records.
Interview: Organizational personnel with security training record retention responsibilities.

Audit and Accountability (AU) – Technical

Table 29. AU-1: Audit and Accountability Policy and Procedures

<table>
<tr><th colspan="3">AU-1: Audit and Accountability Policy and Procedures</th></tr>
<tr><td colspan="3"><b>Control</b></td></tr>
<tr><td colspan="3">The organization develops, disseminates, and reviews/updates within every three-hundred-sixty-five (365) days:
a. A formal, documented audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
b. Formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.</td></tr>
<tr><td colspan="3"><b>Guidance</b></td></tr>
<tr><td colspan="3">This control is intended to produce the policy and procedures that are required for the effective implementation of security controls and control enhancements in the audit and accountability family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The audit and accountability policy can be included as part of the general information security policy for the organization. Audit and accountability procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the audit and accountability policy.</td></tr>
<tr><td><b>Applicability:</b> Exchanges</td><td><b>Reference(s):</b> IRS-1075: 9.3</td><td><b>Related Control Requirements:</b></td></tr>
<tr><td colspan="3"><b>Assessment Procedure: AU-1.1</b></td></tr>
<tr><td colspan="3"><b>Assessment Objective</b></td></tr>
<tr><td colspan="3">Determine if:</td></tr>
<tr><td colspan="3">(i) the organization develops and formally documents audit and accountability policy;
(ii) the organization audit and accountability policy addresses:
– purpose;
– scope;
– roles and responsibilities;
– management commitment;
– coordination among organizational entities;
– compliance;
(iii) the organization disseminates formal documented audit and accountability policy to elements within the organization having associated audit and accountability roles and responsibilities;
(iv) the organization develops and formally documents audit and accountability procedures;
(v) the organization audit and accountability procedures facilitate implementation of the audit and accountability policy and associated audit and accountability controls;
(vi) the organization disseminates formal documented audit and accountability procedures to elements within the organization having associated audit and accountability roles and responsibilities.
(vii) the organization reviews/updates the audit and accountability policy and procedures within every three-hundred-sixty-five (365) days.</td></tr>
<tr><td colspan="3"><b>Assessment Methods and Objects</b></td></tr>
<tr><td colspan="3"><b>Examine:</b> Audit and accountability policy and procedures; other relevant documents or records.</td></tr>
<tr><td colspan="3"><b>Interview:</b> Organizational personnel with audit and accountability responsibilities.</td></tr>
</table>

Table 30. AU-2: Auditable Events

AU-2: Auditable Events

Control

The organization:

a. Determines, based on a risk assessment and mission/business needs, that the information system must be capable of auditing the list of auditable events specified in the Implementation Standards;
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; and
c. Determines, based on current threat information and ongoing assessment of risk, which events require auditing on a continuous basis and which events require auditing in response to specific situations.

For FTI: Audit logs must enable tracking activities taking place on the system. Pub 1075, Exhibit 9, System Audit Management Guidelines, contains requirements for creating audit-related processes at both the application, auditing must be enabled to the extent necessary to capture access, modification, deletion and movement of FTI by each unique user. This auditing requirement also applies to data tables or databases embedded in or residing outside of the application that contain FTI.

Implementation Standards

1. Generate audit records for the following events:
   a. User account management activities,
   b. System shutdown,
   c. System reboot,
   d. System errors,
   e. Application shutdown,
   f. Application restart,
   g. Application errors,
   h. File creation,
   i. File deletion
   j. File modification,
   k. Failed and successful log-ons,
   l. Security policy modifications, and
   m. Use of administrator privileges.
2. Enable logging for perimeter devices, including firewalls and routers.
   a. Log packet screening denials originating from un-trusted networks,
   b. Packet screening denials originating from trusted networks,
   c. User account management,
   d. Modification of packet filters,
   e. Application errors,
   f. System shutdown and reboot,
   g. System errors, and
   h. Modification of proxy services.
3. Verify that proper logging is enabled in order to audit administrator activities.

For FTI: Generate audit records for the following events in addition to those specified in other controls, plus those bolded above:

a. All successful and unsuccessful authorization attempts;
b. All changes to logical access control authorities (e.g., rights, permissions);
c. All system changes with the potential to compromise the integrity of audit policy configurations, security policy configurations and audit record generation services;
d. The audit trail shall capture the enabling or disabling of audit report generation services;
e. The audit trail shall capture command line changes, batch file changes and queries made to the system (e.g., operating system, application, and database).

AU-2: Auditable Events		
Guidance		
The purpose of this control is for the organization to identify events which need to be auditable as significant and relevant to the security of the information system; giving an overall system requirement in order to meet ongoing and specific audit needs. To balance auditing requirements with other information system needs, this control also requires identifying that subset of auditable events that are to be audited at a given point in time. For example, the organization may determine that the information system 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 extreme burden on system performance. In addition, audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the right level of abstraction for audit record generation is a critical aspect of an audit capability and can facilitate the identification of root causes to problems.		
Applicability: Exchanges	**Reference(s):** HIPAA: 164.308(a)(5)(ii)(C), 164.312(b); IRS-1075: 9.3, Exhibit 9	**Related Control Requirements:** AU-4
Assessment Procedure: AU-2.1		
Assessment Objective		
Determine if:		
(i) the organization determines, based on a risk assessment and mission/business needs, that the information system must be capable of auditing the list of auditable events specified in the Implementation Standards; (ii) the organization coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and help guide the selection of auditable events; (iii) the organization provides a rationale for why the list of auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; (iv) the organization defines in the System Security Plan, explicitly or by reference, information system auditable events; (v) the organization defines the subset of auditable events defined in (a) that are to be audited within the information system and (b) the frequency of (or situation requiring) auditing for each identified event; (vi) the organization determines, based on current threat information and ongoing assessment of risk, the subset of auditable events defined in (a) to be audited within the information system, and (b) the frequency of (or situation requiring) auditing for each identified event; (vii) the organization meets all the requirements specified in the applicable implementation standard(s).		
Assessment Methods and Objects		
Examine: Audit and accountability policy; procedures addressing auditable events; security plan; information system configuration settings and associated documentation; information system audit records; list of information system auditable events; other relevant documents or records.		
Interview: Organizational personnel with auditing and accountability responsibilities.		

Table 31. AU-2(4): Privileged Functions Execution Audit

AU-2(4): Privileged Functions Execution Audit		
Control		
The organization includes execution of privileged functions in the list of events to be audited by the information system, including administrator and user account activities, failed and successful log-on, security policy modifications, use of administrator privileges, system shutdowns, reboots, errors, and access authorizations.		
Applicability: Exchanges	**Reference(s):**	**Related Control Requirements:**
Assessment Procedure: AU-2(4).1		
Assessment Objective		
Determine if the organization includes execution of privileged functions in the list of events to be audited by the information system.		
Assessment Methods and Objects		

AU-2(4): Privileged Functions Execution Audit
Examine: Audit and accountability policy; procedures addressing auditable events; information system configuration settings and associated documentation; list of organization-defined auditable events; list of privileged security functions; other relevant documents or records.

Table 32. AU-3: Content of Audit Records

AU-3: Content of Audit Records		
Control		
The information system produces audit records that contain sufficient information to, at a minimum, establish what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event.		
Implementation Standards		
1. (For PHI only) Record disclosures of sensitive information, including protected health and financial information. Log information type, date, time, receiving party, and releasing party. Verify within every ninety (90) days for each extract that the data is erased or its use is still required.		
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.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.3	**Related Control Requirements:**
Assessment Procedure: AU-3.1		
Assessment Objective		
Determine if:		
(i) the information system produces audit records that contain sufficient information to, at a minimum, establish: – what type of event occurred; – when (date and time) the event occurred; – where the event occurred; – the source of the event; – the outcome (success or failure) of the event; – the identity of any user/subject associated with the event. (ii) the organization meets all the requirements specified in the applicable implementation standard(s).		
Assessment Methods and Objects		
Examine: Audit and accountability policy; procedures addressing content of audit records; list of organization-defined auditable events; information system audit records; information system incident reports; other relevant documents or records.		

Table 33. AU-3(1): Audit Detail Information Capability

AU-3(1): Audit Detail Information Capability		
Control		
The information system includes the capability to include more detailed information in the audit records for audit events identified by type, location, or subject.		
Guidance		
An example of detailed information that the organization may require in audit records is full-text recording of privileged commands or the individual identities of group account users.		
Applicability:	**Reference(s):**	**Related Control Requirements:**

AU-3(1): Audit Detail Information Capability		
Exchanges		
Assessment Procedure: AU-3(1).1		
Assessment Objective		
Determine if:		
(i) the organization defines the additional, more detailed information to be included in audit records for audit events identified by type, location, or subject; (ii) the information system includes the organization-defined additional, more detailed information in the audit records for audit events identified by type, location, or subject.		
Assessment Methods and Objects		
Examine: Audit and accountability policy; procedures addressing content of audit records; list of organization-defined auditable events; information system design documentation; security plan; information system configuration settings and associated documentation; other relevant documents or records.		

Table 34. AU-4: Audit Storage Capacity

AU-4: Audit Storage Capacity		
Control		
The organization allocates audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.		
Guidance		
The organization considers the types of auditing to be performed and the audit processing requirements when allocating audit storage capacity.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.3	**Related Control Requirements:** AU-2, AU-5, AU-6, SI-4
Assessment Procedure: AU-4.1		
Assessment Objective		
Determine if:		
(i) the organization allocates audit record storage capacity; (ii) the organization configures auditing to reduce the likelihood of audit record storage capacity being exceeded.		
Assessment Methods and Objects		
Examine: Audit and accountability policy; procedures addressing audit storage capacity; information system design documentation; organization-defined audit record storage capacity for information system components that store audit records; list of organization-defined auditable events; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.		

Table 35. AU-5: Response to Audit Processing Failures

AU-5: Response to Audit Processing Failures
Control
The information system: a. Alerts designated organizational officials in the event of an audit processing failure; and b. Takes the following additional actions in response to an audit failure or audit storage capacity issue: – Shutdown the information system, – Stop generating audit records, or – Overwrite the oldest records, in the case that storage media is unavailable. For FTI: Shutting down the system, stopping the generation of audit reports or overwriting the oldest records is not an appropriate action.

<table>
<tr><th colspan="3">AU-5: Response to Audit Processing Failures</th></tr>
<tr><td colspan="3"><b>Guidance</b></td></tr>
<tr><td colspan="3">Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.</td></tr>
<tr><td><b>Applicability:</b> Exchanges</td><td><b>Reference(s):</b> IRS-1075: 3.0, 9.3</td><td><b>Related Control Requirements:</b> AU-4</td></tr>
<tr><td colspan="3"><b>Assessment Procedure: AU-5.1</b></td></tr>
<tr><td colspan="3"><b>Assessment Objective</b></td></tr>
<tr><td colspan="3">Determine if:</td></tr>
<tr><td colspan="3">(i) the organization defines designated organizational officials to be alerted in the event of an audit processing failure;
(ii) the organization defines in the System Security Plan, explicitly or by reference, personnel to be notified in case of an audit processing failure;
(iii) the organization defines additional actions to be taken in the event of an audit processing failure;
(iv) the information system takes the additional organization-defined actions in the event of an audit processing failure.</td></tr>
<tr><td colspan="3"><b>Assessment Methods and Objects</b></td></tr>
<tr><td colspan="3"><b>Examine:</b> Audit and accountability policy; procedures addressing response to audit processing failures; information system design documentation; security plan; information system configuration settings and associated documentation; list of personnel to be notified in case of an audit processing failure; information system audit records; other relevant documents or records.</td></tr>
</table>

Table 36. AU-6: Audit Review, Analysis, and Reporting

<table>
<tr><th>AU-6: Audit Review, Analysis, and Reporting</th></tr>
<tr><td><b>Control</b></td></tr>
<tr><td>The organization:
a. Reviews and analyzes information system audit records regularly for indications of inappropriate or unusual activity, and reports findings to designated organizational officials; and
b. Adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk to CMS operations, CMS assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.
For FTI: All requests for return information, including receipt and/or disposal of returns or return information, shall be maintained in a log.</td></tr>
<tr><td><b>Implementation Standards</b></td></tr>
<tr><td>2. Review system records for initialization sequences, log-ons and errors; system processes and performance; and system resources utilization to determine anomalies on demand but no less than once within a twenty-four (24) hour period. Generate alert notification for technical personnel review and assessment.
3. Review network traffic, bandwidth utilization rates, alert notifications, and border defense devices to determine anomalies on demand but no less than once within a twenty-four (24) hour period. Generate alerts for technical personnel review and assessment.
4. Investigate suspicious activity or suspected violations on the information system, report findings to appropriate officials and take appropriate action.
5. Use automated utilities to review audit records at least once every seven (7) days for unusual, unexpected, or suspicious behavior.
6. Inspect administrator groups on demand but at least once every fourteen (14) days to ensure unauthorized administrator accounts have not been created.
7. Perform manual reviews of system audit records randomly on demand but at least once every thirty (30) days.</td></tr>
<tr><td><b>Guidance</b></td></tr>
<tr><td>Organizations increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to operations, assets, or individuals based on law enforcement information,</td></tr>
</table>

AU-6: Audit Review, Analysis, and Reporting		
intelligence information, or other credible sources of information.		
Applicability: Exchanges	**Reference(s):** HIPAA: 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(C), 164.312(b); IRS-1075: 3.0, 9.3	**Related Control Requirements:** AU-4, IR-4
Assessment Procedure: AU-6.1		
Assessment Objective		
Determine if:		
(i) the organization reviews and analyzes information system audit records for indications of inappropriate or unusual activity in accordance with the organization-defined frequency; (ii) the organization adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk to system operations, system assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information; (iii) the organization report findings of inappropriate/unusual activities, to designated organizational officials; (iv) the organization meets all the requirements specified in the applicable implementation standard(s).		
Assessment Methods and Objects		
Examine: Audit and accountability policy; procedures addressing audit review, analysis, and reporting; reports of audit findings; records of actions taken in response to reviews/analyses of audit records; other relevant documents or records.		
Examine: Logs for requests of FTI include receipt and/or disposal or FTI information is returned.		
Interview: Organizational personnel with information system audit review, analysis, and reporting responsibilities.		
Interview: Organizational personnel responsible for handling FTI.		
Assessment Procedure: AU-6.2		
Assessment Objective		
Determine if the organization adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk to organizational operations, organizational assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.		
Assessment Methods and Objects		
Examine: Audit and accountability policy; procedures addressing audit review, analysis, and reporting; threat information documentation from law enforcement, intelligence community, or other sources; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.		
Interview: Organizational personnel with information system audit review, analysis, and reporting responsibilities.		

Table 37. AU-6(1): Audit Review, Analysis, and Reporting

AU-6(1): Audit Review, Analysis, and Reporting		
Control		
The information system integrates audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.		
Guidance		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.3	**Related Control Requirements:**
Assessment Procedure: AU-6(1).1		
Assessment Objective		
Determine if the information system integrates audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.		

AU-6(1): Audit Review, Analysis, and Reporting
Assessment Methods and Objects
Examine: Audit and accountability policy; procedures addressing audit review, analysis, and reporting; information system design documentation; information system configuration settings and associated documentation; procedures for investigating and responding to suspicious activities; other relevant documents or records.
Interview: Organizational personnel with information system audit review, analysis, and reporting responsibilities.

Table 38. AU-7: Audit Reduction and Report Generation

AU-7: Audit Reduction and Report Generation		
Control		
The information system provides an audit reduction and report generation capability.		
Guidance		
An audit reduction and report generation capability provides support for near real-time audit review, analysis, and reporting requirements described in AU-6 and after-the-fact investigations of security incidents. Audit reduction and reporting tools do not alter original audit records.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.3	**Related Control Requirements:** AU-6
Assessment Procedure: AU-7.1		
Assessment Objective		
Determine if the information system provides an audit reduction and report generation capability.		
Assessment Methods and Objects		
Examine: Audit and accountability policy; procedures addressing audit reduction and report generation; information system design documentation; audit reduction, review, and reporting tools; information system audit records; other relevant documents or records.		
Interview: Organizational personnel with information system audit review, analysis, and reporting responsibilities.		

Table 39. AU-7(1): Audit Reduction and Report Generation

AU-7(1): Audit Reduction and Report Generation		
Control		
The information system provides the capability to automatically process audit records for events of interest based on selectable event criteria.		
Guidance		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.3	**Related Control Requirements:**
Assessment Procedure: AU-7(1).1		
Assessment Objective		
Determine if the information system provides the capability to automatically process audit records for events of interest based on selectable event criteria.		
Assessment Methods and Objects		
Examine: Audit and accountability policy; procedures addressing audit reduction and report generation; information system design documentation; information system configuration settings and associated documentation; documented criteria for selectable events to audit; audit reduction, review, and reporting tools; information system audit records; other relevant documents or records.		

Table 40. AU-8: Time Stamps

<table>
<tr><th colspan="3">AU-8: Time Stamps</th></tr>
<tr><td colspan="3"><b>Control</b></td></tr>
<tr><td colspan="3">The information system uses internal system clocks to generate time stamps for audit records.</td></tr>
<tr><td colspan="3"><b>Guidance</b></td></tr>
<tr><td colspan="3">Time stamps generated by the information system include both date and time. The time may be expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC.</td></tr>
<tr><td><b>Applicability:</b> Exchanges</td><td><b>Reference(s):</b> IRS-1075: 9.3</td><td><b>Related Control Requirements:</b> AU-3</td></tr>
<tr><td colspan="3"><b>Assessment Procedure: AU-8.1</b></td></tr>
<tr><td colspan="3"><b>Assessment Objective</b></td></tr>
<tr><td colspan="3">Determine if the information system uses internal system clocks to generate time stamps for audit records.</td></tr>
<tr><td colspan="3"><b>Assessment Methods and Objects</b></td></tr>
<tr><td colspan="3"><b>Examine:</b> Audit and accountability policy; procedures addressing time stamp generation; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.</td></tr>
</table>

Table 41. AU-8(1): Time Stamps

<table>
<tr><th colspan="3">AU-8(1): Time Stamps</th></tr>
<tr><td colspan="3"><b>Control</b></td></tr>
<tr><td colspan="3">The information system synchronizes internal information system clocks daily and at system boot.</td></tr>
<tr><td colspan="3"><b>Guidance</b></td></tr>
<tr><td colspan="3"></td></tr>
<tr><td><b>Applicability:</b> Exchanges</td><td><b>Reference(s):</b> IRS-1075: 9.3</td><td><b>Related Control Requirements:</b></td></tr>
<tr><td colspan="3"><b>Assessment Procedure: AU-8(1).1</b></td></tr>
<tr><td colspan="3"><b>Assessment Objective</b></td></tr>
<tr><td colspan="3">Determine if:</td></tr>
<tr><td colspan="3">(i) the organization defines the frequency of internal clock synchronization for the information system;
(ii) the organization defines the authoritative time source for internal clock synchronization; and
(iii) the organization synchronizes internal information system clocks with the organization-defined authoritative time source in accordance with the organization-defined frequency.</td></tr>
<tr><td colspan="3"><b>Assessment Methods and Objects</b></td></tr>
<tr><td colspan="3"><b>Examine:</b> Audit and accountability policy; procedures addressing time stamp generation; security plan; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.</td></tr>
</table>

Table 42. AU-9: Protection of Audit Information

<table>
<tr><th>AU-9: Protection of Audit Information</th></tr>
<tr><td><b>Control</b></td></tr>
<tr><td>The information system protects audit information and audit tools from unauthorized access, modification, and deletion.</td></tr>
<tr><td><b>Guidance</b></td></tr>
<tr><td>Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully</td></tr>
</table>

AU-9: Protection of Audit Information		
audit information system activity.		
Applicability: Exchanges	**Reference(s)**: IRS-1075: 9.3	**Related Control Requirements:**
Assessment Procedure: AU-9.1		
Assessment Objective		

Determine if the information system protects audit information and audit tools from unauthorized:
(i) access;
(ii) modification;
(iii) deletion.		

Assessment Methods and Objects		
Examine: Audit and accountability policy; procedures addressing protection of audit information; access control policy and procedures; information system design documentation; information system configuration settings and associated documentation, information system audit records; audit tools; other relevant documents or records.		

Table 43. AU-10: Non-Repudiation

AU-10: Non-Repudiation		
Control		
The information system protects against an individual falsely denying having performed a particular action.		
Guidance		
Examples of particular actions taken by individuals include creating information, sending a message, approving information (e.g., indicating concurrence or signing a contract), and receiving a message. Non-repudiation protects individuals against later claims by an author of not having authored a particular document, a sender of not having transmitted a message, a receiver of not having received a message, or a signatory of not having signed a document. Non-repudiation services can be used to determine if information originated from an individual, or if an individual took specific actions (e.g., sending an email, signing a contract, approving a procurement request) or received specific information. Non-repudiation services are obtained by employing various techniques or mechanisms (e.g., digital signatures, digital message receipts).		
Applicability: Exchanges	**Reference(s)**:	**Related Control Requirements:**
Assessment Procedure: AU-10.1		
Assessment Objective		
Determine if the information system protects against an individual falsely denying having performed a particular action.		
Assessment Methods and Objects		
Examine: Audit and accountability policy; procedures addressing non-repudiation; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.		

Table 44. AU-11: Audit Record Retention

AU-11: Audit Record Retention
Control
The organization retains audit records for ninety (90) days and archive old records for one (1) year to provide support for after-the-fact investigations of security incidents and to meet regulatory and information retention requirements. For FTI: 1. Employ a permanent system of standardized records of request for disclosure of FTI and maintain the

AU-11: Audit Record Retention		
records for five (5) years or the applicable records control schedule, whichever is longer. 2. To support the audit of FTI activities, all organizations must ensure that audit information is archived for six (6) years to enable the recreation of computer-related accesses to both the operating system and to the application wherever FTI is stored.		
Implementation Standard		
1. (For PII only) Audit inspection reports, including a record of corrective actions, shall be retained by the organization for a minimum of three (3) years from the date the inspection was completed.		
Guidance		
The organization retains 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, subpoena, and law enforcement actions. Standard categorizations of audit records relative to such types of actions and standard response processes for each type of action are developed and disseminated. The National Archives and Records Administration (NARA) General Records Schedules (GRS) provide federal policy on record retention.		
Applicability: Exchanges	**Reference(s)**: IRS-1075: 3.1, 9.3	**Related Control Requirements:**
Assessment Procedure: AU-11.1		
Assessment Objective		
Determine if:		
(i) the organization defines the retention period for audit records; (ii) the retention period for audit records is consistent with the records retention policy; and (iii) the organization retains audit records for the organization-defined time period consistent with the records retention policy to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.		
Assessment Methods and Objects		
Examine: Audit and accountability policy; procedures addressing audit record retention; security plan; organization-defined retention period for audit records; information system audit records; other relevant documents or records.		
Interview: Organizational personnel with information system audit record retention responsibilities.		

Table 45. AU-12: Audit Generation

AU-12: Audit Generation
Control
The information system: a. Provides audit record generation capability for the following events in addition to those specified in other controls: – All successful and unsuccessful authorization attempts. – All changes to logical access control authorities (e.g., rights, permissions). – All system changes with the potential to compromise the integrity of audit policy configurations, security policy configurations and audit record generation services. – The audit trail shall capture the enabling or disabling of audit report generation services. – The audit trail shall capture command line changes, batch file changes and queries made to the system (e.g., operating system, application, and database). b. Allows designated organizational personnel to select which auditable events are to be audited by specific components of the system; and c. Generates audit records for the list of audited events defined in AU-2 with the content as defined in AU-3.
Guidance
Audits records can be generated from various components within the information system. The list of audited events is the set of events for which audits are to be generated. This set of events is typically a subset of the list of all events for which the system is capable of generating audit records (i.e., auditable events).

AU-12: Audit Generation		
Applicability: Exchanges	**Reference(s**): IRS-1075: 9.3	**Related Control Requirements:** AU-2, AU-3
Assessment Procedure: AU-12.1		
Assessment Objective		
Determine if:		
(i) the organization defines the information system components that provide audit record generation capability for the list of auditable events defined in AU-2; (ii) the information system provides audit record generation capability, at organization-defined information system components, for the list of auditable events defined in AU-2; (iii) the information system allows designated organizational personnel to select which auditable events are to be audited by specific components of the system; and (iv) the information system generates audit records for the list of audited events defined in AU-2 with the content as defined in AU-3.		
Assessment Methods and Objects		
Assessment Methods And Objects		
Examine: Audit and accountability policy; procedures addressing audit record generation; security plan; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.		
Interview: Organizational personnel with information system audit record generation responsibilities.		

Table 46. AU-12(1): Audit Generation

AU-12(1): Audit Generation		
Control		
The information system compiles audit records from multiple components throughout the system into a system-wide (logical or physical) time-correlated audit trail.		
Guidance		
The audit trail is time-correlated if the time stamp in the individual audit records can be reliably related to the time stamp in other audit records to achieve a time ordering of the records within the organization-defined tolerance.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.3	**Related Control Requirements:**
Assessment Procedure: AU-12(1).1		
Assessment Objective		
Determine if:		
(i) the information system produces a system-wide (logical or physical) audit trail of information system audit records; (ii) the organization defines the information system components from which audit records are to be compiled into the system-wide audit trail; (iii) the information system compiles audit records from organization-defined information system components into the system-wide audit trail; (iv) the organization defines the acceptable level of tolerance for relationship between time stamps of individual records in the system-wide audit trail; and (v) the system-wide audit trail is time-correlated to within the organization-defined level of tolerance to achieve a time ordering of audit records.		
Assessment Methods and Objects		
Examine: Audit and accountability policy; procedures addressing audit record generation; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.		

Security and Assessment Authorization (CA) – Management

Table 47. CA-1: Security Assessment and Authorization Policies and Procedures

CA-1: Security Assessment and Authorization Policies and Procedures		
Control		
The organization develops, disseminates, and reviews/updates within every three-hundred-sixty-five (365) days: a. Formal, documented security assessment and authorization policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the security assessment and authorization policies and associated security assessment and authorization controls.		
Guidance		
This control is intended to produce the policy and procedures that are required for the effective implementation of security controls and control enhancements in the security assessment and authorization family [formerly called Certification and Accreditation (C&A) family and process]. The policies and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The security assessment/authorization policies can be included as part of the general information security policy for the organization. Security assessment/authorization procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the security assessment and authorization policy.		
Applicability: Exchanges	**Reference(s):** HIPAA: 164.308(a)(8); HSPD 7: F(19); IRS-1075: 9.5	**Related Control Requirements:**
Assessment Procedure: CA-1.1		
Assessment Objective		
Determine if:		
(i) the organization develops and formally documents security assessment and authorization policy; (ii) the organization security assessment and authorization policy addresses: – purpose; – scope; – roles and responsibilities; – management commitment; – coordination among organizational entities; – compliance; (iii) the organization disseminates formal documented security assessment and authorization policy to elements within the organization having associated security assessment and authorization roles and responsibilities; (iv) the organization develops and formally documents security assessment and authorization procedures; (v) the organization security assessment and authorization procedures facilitate implementation of the security assessment and authorization policy and associated security assessment and authorization controls; (vi) the organization disseminates formal documented security assessment and authorization procedures to elements within the organization having associated security assessment and authorization roles and responsibilities; (vii) the organization reviews/updates the security assessment and authorization policies and procedures within every three-hundred-sixty-five (365) days.		
Assessment Methods and Objects		
Examine: Security assessment and authorization policies and procedures; other relevant documents or records.		
Interview: Organizational personnel with security assessment and authorization responsibilities.		

Table 48. CA-2: Security Assessments

CA-2: Security Assessments

Control

The organization:

a. Develops a security assessment plan that describes the scope of the assessment including:
   - Security controls and control enhancements under assessment;
   - Assessment procedures to be used to determine security control effectiveness; and
   - Assessment environment, assessment team, and assessment roles and responsibilities;

b. Assesses the security controls in the information system within every three-hundred-sixty-five (365) days in accordance with the *Catalog of Minimum Acceptable Risk Controls for Exchanges – Exchange Reference Architecture Supplement* to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system;

c. Produces a security assessment report that documents the results of the assessment; and

d. Provides the results of the security control assessment within every three-hundred-sixty-five (365) days, in writing, to the Business Owner who is responsible for reviewing the assessment documentation and updating system security documentation where necessary to reflect any changes to the system.

For FTI: The agency shall conduct, periodically, but at least annually, an assessment of the security controls in the systems that receive, store, process or transmit FTI.

Implementation Standards

1. A security assessment of all security controls must be conducted prior to issuing the initial authority to operate for all newly implemented systems.
2. The annual security assessment requirement mandated by CMS requires all Minimum Security Controls for States attributable to a system or application to be assessed over a 3-year period. To meet this requirement, a subset of the *Minimum Acceptable Risk Controls for Exchanges – Exchange Reference Architecture Supplement* shall be tested each year so that all security controls are tested during a 3-year period.
3. The Business Owner notifies the CISO within thirty (30) days whenever updates are made to system security authorization artifacts or significant role changes occur (e.g., Business Owner, System Developer/Maintainer, ISSO).

Guidance

The organization assesses the security controls in an information system as part of: (i) security authorization or reauthorization; (ii) meeting CMS' required annual assessments; (iii) continuous monitoring; and (iv) testing/evaluation of the information system as part of the system development life cycle process. The assessment report documents the assessment results in sufficient detail as deemed necessary by the organization, to determine the accuracy and completeness of the report and whether the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements of the information system. The required (at least) annual security control assessments should not be interpreted by organizations as adding additional assessment requirements to those requirements already in place in the security authorization process. To satisfy the annual assessment requirement, organizations can draw upon the security control assessment results from any of the following sources, including but not limited to: (i) assessments conducted as part of an information system authorization or reauthorization process; (ii) continuous monitoring (see CA-7); or (iii) testing and evaluation of an information system as part of the ongoing system development life cycle (provided that the testing and evaluation results are current and relevant to the determination of security control effectiveness). Existing security control assessment results are reused to the extent that they are still valid and are supplemented with additional assessments as needed.

Subsequent to the initial authorization of the information system, the organization assesses a subset of the security controls annually during continuous monitoring. The organization establishes the security control selection criteria and subsequently selects a subset of the security controls within the information system and its environment of operation for assessment. Those security controls that are the most volatile (i.e., controls most affected by ongoing changes to the information system or its environment of operation) or deemed critical to protecting Exchange operations and assets, individuals, other organizations, and the Nation are assessed more frequently in accordance with an organizational assessment of risk. All other controls are assessed at least once during the information system's three-year authorization cycle. The organization can use the current year's assessment results from any of the above sources to meet the annual assessment requirement provided that the results are current, valid, and

CA-2: Security Assessments		
relevant to determining security control effectiveness. External audits (e.g., audits conducted by external entities such as regulatory agencies) are outside the scope of this control.		
Applicability: Exchanges	**Reference(s):** HIPAA: 164.306(e), 164.308(a)(8); F(19); IRS-1075: 9.5	**Related Control Requirements:** CA-7
Assessment Procedure: CA-2.1		
Assessment Objective		
Determine if:		
(i) the organization develops a security assessment plan for the information system; – the security assessment plan describes the scope of the assessment including: – security controls and control enhancements under assessment; – assessment procedures to be used to determine security control effectiveness; (ii) assessment environment, assessment team, and assessment roles and responsibilities. (iii) the organization meets all the requirements specified in the applicable implementation standard(s).		
Assessment Methods and Objects		
Examine: Security assessment policy; procedures addressing security assessments; security plan; security assessment plan; assessment evidence; other relevant documents or records.		
Assessment Procedure: CA-2.2		
Assessment Objective		
Determine if:		
(i) the organization assesses the security controls in the information system within every three-hundred-sixty-five (365) days in accordance with the *Minimum Acceptable Risk Controls for Exchanges – Exchange Reference Architecture Supplement,* to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system; (ii) the organization provides the results of the security control assessment within every 365 days, in writing, to the Business Owner; (iii) the Business Owner reviews the assessment documentation and updates system security documentation where necessary to reflect any changes to the system; (iv) the results of the security control assessment are provided, in writing, to the authorizing official or authorizing official designated representative.		
Assessment Method and Objects		
Examine: Security assessment and authorization policy; procedures addressing security assessments; security plan; security assessment plan; security assessment report; security assessment evidence; plan of action and milestones; other relevant documents or records.		
Interview: Organizational personnel with security assessment responsibilities.		

Table 49. CA-2(1): Employ Independent Assessor

CA-2(1): Employ Independent Assessor		
Control		
The organization employs an independent assessor or assessment team to conduct an assessment of the security controls in the Exchange information system.		
Guidance		
An independent assessor or assessment team is any individual or group capable of conducting an impartial assessment of an Exchange information system. Impartiality implies that the assessors are free from any perceived or actual conflicts of interest with respect to the developmental, operational, and/or management chain associated with the information system or to the determination of security control effectiveness. Independent security assessment services can be obtained from other elements within the organization or can be contracted to a public or private sector entity outside of the organization. Contracted assessment services are considered independent if the information system owner is not directly involved in the contracting process or cannot unduly influence the impartiality of the assessor or assessment team conducting the assessment of the security controls in the information system. In special situations, for example when the organization that owns the information system is small or the organizational structure requires that the assessment be accomplished by individuals that are in the developmental, operational, and/or management chain of the system owner, independence in the assessment process can be achieved by ensuring that the assessment results are carefully reviewed and analyzed by an independent team of experts to validate the completeness, accuracy, integrity, and reliability of the results.		
Applicability: Exchanges	**Reference(s):**	**Related Control Requirements:**
Assessment Procedure: CA-2(1).1		
Assessment Objective		
Determine if the organization employs an independent assessor or assessment team to conduct an assessment of the security controls in the information system.		
Assessment Methods and Objects		
Examine: Security assessment and authorization policy; procedures addressing security assessments; security authorization package (including security plan, security assessment report, plan of action and milestones, authorization statement); other relevant documents or records.		
Interview: Organizational personnel with security assessment responsibilities.		

Table 50. CA-3: Information System Connections

CA-3: Information System Connections
Control
The organization: a. Authorizes connections from the Exchange information system to other information systems outside of the authorization boundary through the use of Interconnection Security Agreements; b, Documents, for each connection, the interface characteristics, security requirements, and the nature of the information communicated; and c. Monitors the information system connections on an ongoing basis verifying enforcement of security requirements.
Implementation Standards
1. Record each system interconnection in the System Security Plan (SSP) and Information Security (IS) Risk Assessment (RA) for the system that is connected to the remote location.
Guidance
This control applies to dedicated connections between information systems and does not apply to transitory, user-controlled connections such as email and website browsing. The organization carefully considers the risks that may be introduced when information systems are connected to other systems with different security requirements and security controls, both within the organization and external to the organization. Authorizing officials determine the risk associated with each connection and the appropriate controls employed. If the interconnecting systems have the

<table>
<tr><th colspan="3">CA-3: Information System Connections</th></tr>
<tr><td colspan="3">same authorizing official, an Interconnection Security Agreement is not required. Rather, the interface characteristics between the interconnecting information systems are described in the security plans for the respective systems. If the interconnecting systems have different authorizing officials but the authorizing officials are in the same organization, the organization determines whether an Interconnection Security Agreement is required, or alternatively, the interface characteristics between systems are described in the security plans of the respective systems. Instead of developing an Interconnection Security Agreement, organizations may choose to incorporate this information into a formal contract, especially if the interconnection is to be established between the system and a nonfederal (private sector) organization. In every case, documenting the interface characteristics is required, yet the formality and approval process vary considerably even though all accomplish the same fundamental objective of managing the risk being incurred by the interconnection of the information systems. Risk considerations also include information systems sharing the same networks. Information systems may be identified and authenticated as devices in accordance with organizational policy.</td></tr>
<tr><td><b>Applicability:</b> Exchanges</td><td><b>Reference(s):</b> IRS-1075: 9.5</td><td><b>Related Control Requirements:</b> SA-9, SC-7</td></tr>
<tr><td colspan="3"><b>Assessment Procedure: CA-3.1</b></td></tr>
<tr><td colspan="3"><b>Assessment Objective</b></td></tr>
<tr><td colspan="3">Determine if:</td></tr>
<tr><td colspan="3">(i) the organization identifies connections to external information systems (i.e., information systems outside of the authorization boundary);
(ii) the organization authorizes connections from the information system to external information systems through the use of Interconnection Security Agreements;
(iii) the organization documents, for each connection, the interface characteristics, security requirements, and the nature of the information communicated;
(iv) the organization monitors the information system connections on an ongoing basis to verify enforcement of security requirements.
(v) the organization meets all the requirements specified in the applicable implementation standard(s).</td></tr>
<tr><td colspan="3"><b>Assessment Methods and Objects</b></td></tr>
<tr><td colspan="3"><b>Examine:</b> Access control policy; procedures addressing information system connections; system and communications protection policy; information system interconnection security agreements; security plan; information system design documentation; security assessment report; plan of action and milestones; other relevant documents or records.</td></tr>
<tr><td colspan="3"><b>Interview:</b> Organizational personnel with responsibility for developing, implementing, or approving information system interconnection agreements.</td></tr>
</table>

Table 51. CA-5: Plan of Action and Milestones (POA&M)

CA-5: Plan of Action and Milestones (POA&M)
Control
The organization: a. Develops and submits a Plan of Action and Milestones (POA&M) for the information system within thirty (30) days of the final results for every internal/external audit/review or test (e.g., ST&E, penetration test) 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 and submits existing POA&M monthly until all the findings are resolved based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.
Implementation Standards
For FTI: The agency must submit an updated Corrective Action Plan (CAP) twice each year to address corrective actions identified during an on-site safeguards review until all findings are closed. The CAP is submitted as an attachment to the SAR, and on the CAP due date which is six months from the scheduled SAR due date.
Guidance
The plan of action and milestones is a key document in the security authorization package and is subject to federal

CA-5: Plan of Action and Milestones (POA&M)		
reporting requirements established by OMB.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 7.5, 9.5	**Related Control Requirements:** PM-4
Assessment Procedure: CA-5.1		
Assessment Objective		
Determine if:		
(i) the organization develops a plan of action and milestones for the information system; (ii) the plan of action and milestones documents 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; (iii) the organization defines the frequency of plan of action and milestone updates; and (iv) the organization updates the plan of action and milestones at an organization-defined frequency with findings from: – security controls assessments; – security impact analyses; and – continuous monitoring activities.		
Assessment Methods and Objects		
Examine: Security assessment and authorization policy; procedures addressing plan of action and milestones; security plan; security assessment plan; security assessment report; assessment evidence; plan of action and milestones; other relevant documents or records.		
Interview: Organizational personnel with plan of action and milestones development and implementation responsibilities.		

Table 52. CA-5(1): Plan of Action and Milestones (POA&M)

CA-5(1): Plan of Action and Milestones (POA&M)		
Control		
The organization employs automated mechanisms to help ensure that the POA&M for the information system is accurate, up to date, and readily available.		
Guidance		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.5	**Related Control Requirements:**
Assessment Procedure: CA-5(1).1		
Assessment Objective		
Determine if the organization employs automated mechanisms to help ensure that the plan of action and milestones for the information system is: (i) accurate; (ii) up to date; and (iii) readily available.		
Assessment Methods and Objects		
Examine: Security assessment and authorization policy; procedures addressing plan of action and milestones; information system design documentation, information system configuration settings and associated documentation; plan of action and milestones; other relevant documents or records.		
Interview: Organizational personnel with plan of action and milestones development and implementation responsibilities.		

Table 53. CA-6: Security Authorization

<table>
<tr><th colspan="3">CA-6: Security Authorization</th></tr>
<tr><td colspan="3"><b>Control</b></td></tr>
<tr><td colspan="3">The organization updates the security authorization:
a. At least every three (3) years;
b. When substantial changes are made to the system;
c. When changes in requirements result in the need to process data of a higher sensitivity;
d. When changes occur to authorizing legislation or federal requirements;
e. After the occurrence of a serious security violation which raises questions about the validity of an earlier security authorization; and
f. Prior to expiration of a previous security authorization.
For FTI: Owners of FTI shall accredit the security controls used to protect FTI before initiating operations. This shall be done for any infrastructure associated with FTI. The authorization shall occur every three (3) years or whenever there is a significant change to the control structure. A senior agency official shall sign and approve the authorization.
Note: For Federal agencies that receive FTI, a NIST compliant systems certification (C&A) is required in accordance with FISMA. For state agencies that receive FTI, a third-party accreditation is not required. Instead, these agencies may internally attest in writing that the security controls have been adequately implemented to protect FTI. The accreditation shall occur every three (3) years or whenever there is a significant change to the control structure.</td></tr>
<tr><td colspan="3"><b>Guidance</b></td></tr>
<tr><td colspan="3">Security authorization is the official management decision given by a senior organizational official or executive (i.e., authorizing official) to authorize operation of an information system and to explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls. Authorizing officials typically have budgetary oversight for information systems or are responsible for the mission or business operations supported by the systems. Security authorization is an inherently federal responsibility and therefore, authorizing officials must be federal employees. Through the security authorization process, authorizing officials are accountable for the security risks associated with information system operations. Accordingly, authorizing officials are in management positions with a level of authority commensurate with understanding and accepting such information system-related security risks. Through the employment of a comprehensive continuous monitoring process, the critical information contained in the authorization package (i.e., the security plan (including risk assessment), the security assessment report, and the plan of action and milestones) is updated on an ongoing basis, providing the authorizing official and the information system owner with an up-to-date status of the security state of the information system. To reduce the administrative cost of security reauthorization, the authorizing official uses the results of the continuous monitoring process to the maximum extent possible as the basis for rendering a reauthorization decision. OMB policy requires that federal information systems are reauthorized at least every three years or when there is a significant change to the system. The organization defines what constitutes a significant change to the information system.</td></tr>
<tr><td><b>Applicability:</b> Exchanges</td><td><b>Reference(s):</b> IRS-1075: 9.5</td><td><b>Related Control Requirements:</b> CA-2, CA-7, PM-9, PM-10</td></tr>
<tr><td colspan="3"><b>Assessment Procedure: CA-6.1</b></td></tr>
<tr><td colspan="3"><b>Assessment Objective</b></td></tr>
<tr><td colspan="3">Determine if:</td></tr>
<tr><td colspan="3">(i) the organization assigns a senior-level executive or manager to the role of authorizing official for the information system;
(ii) the authorizing official authorizes the information system for processing before commencing operations;
(iii) the organization defines the frequency of security authorization updates; and
(iv) the organization updates the security authorization in accordance with an organization-defined frequency.</td></tr>
<tr><td colspan="3"><b>Assessment Methods and Objects</b></td></tr>
<tr><td colspan="3"><b>Examine:</b> Security assessment and authorization policy; procedures addressing security authorization; security authorization package (including security plan; security assessment report; plan of action and milestones; authorization statement); other relevant documents or records.</td></tr>
<tr><td colspan="3"><b>Interview:</b> Organizational personnel with security authorization responsibilities.</td></tr>
</table>

Table 54. CA-7: Continuous Monitoring

<table>
<tr><th colspan="3">CA-7: Continuous Monitoring</th></tr>
<tr><td colspan="3"><b>Control</b></td></tr>
<tr><td colspan="3">The organization establishes a continuous monitoring strategy and implements a continuous monitoring program that includes:
a. A configuration management process for the information system and its constituent components;
b. A determination of the security impact of changes to the information system and environment of operation;
c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy; and
d. Reporting the security state of the information system to appropriate organizational officials within every three-hundred-sixty-five (365) days.</td></tr>
<tr><td colspan="3"><b>Guidance</b></td></tr>
<tr><td colspan="3">A continuous monitoring program allows an organization to maintain the security authorization of an information system over time in a highly dynamic environment of operation with changing threats, vulnerabilities, technologies, and missions/business processes. Continuous monitoring of security controls using automated support tools facilitates near real-time risk management and promotes organizational situational awareness with regard to the security state of the information system. The implementation of a continuous monitoring program results in ongoing updates to the security plan, the security assessment report, and the plan of action and milestones, the three principal documents in the security authorization package. A rigorous and well executed continuous monitoring program significantly reduces the level of effort required for the reauthorization of the information system. Continuous monitoring activities are scaled in accordance with the security categorization of the information system.</td></tr>
<tr><td><b>Applicability:</b> Exchanges</td><td><b>Reference(s):</b></td><td><b>Related Control Requirements:</b> CA-2</td></tr>
<tr><td colspan="3"><b>Assessment Procedure: CA-7.1</b></td></tr>
<tr><td colspan="3"><b>Assessment Objective</b></td></tr>
<tr><td colspan="3">Determine if:</td></tr>
<tr><td colspan="3">(i) the organization establishes a continuous monitoring strategy and program;
(ii) the organization defines the frequency for reporting the security state of the information system to appropriate organizational officials;
(iii) the organization defines organizational officials to whom the security state of the information system should be reported;
(iv) the organization implements a continuous monitoring program that includes:
– a configuration management process for the information system and its constituent components;
– a determination of the security impact of changes to the information system and environment of operation;
– ongoing security control assessments in accordance with the organizational continuous monitoring strategy;
– reporting the security state of the information system to appropriate organizational officials in accordance with organization-defined frequency.</td></tr>
<tr><td colspan="3"><b>Assessment Methods and Objects</b></td></tr>
<tr><td colspan="3"><b>Examine:</b> Security assessment and authorization policy; procedures addressing continuous monitoring of information system security controls; procedures addressing configuration management; security plan; security assessment report; plan of action and milestones; information system monitoring records; configuration management records, security impact analyses; status reports; other relevant documents or records.</td></tr>
<tr><td colspan="3"><b>Interview:</b> Organizational personnel with continuous monitoring responsibilities; organizational personnel with configuration management responsibilities.</td></tr>
</table>

Table 55. CA-7(1): Continuous Monitoring

CA-7(1): Continuous Monitoring		
Control		
The use of independent security assessment agents or teams to monitor security controls is not required; however, if the organization employs an independent assessor or assessment team to monitor the security controls in the information system on an ongoing basis, this can be used to satisfy ST&E requirements.		
Guidance		
The organization can extend and maximize the value of the ongoing assessment of security controls during the continuous monitoring process by requiring an independent assessor or team to assess all of the security controls during the information system's three-year authorization cycle. See supplemental guidance for CA-2, enhancement (1), for further information on assessor independence.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.5	**Related Control Requirements:** CA-2, CA-5, CA-6, CM-4
Assessment Procedure: CA-7(1).1		
Assessment Objective		
Determine if the organization employs an independent assessor or assessment team to monitor the security controls in the information system on an ongoing basis.		
Assessment Methods and Objects		
Examine: Security assessment and authorization policy; procedures addressing continuous monitoring of information system security controls; security plan; security assessment report; plan of action and milestones; information system monitoring records; security impact analyses; status reports; other relevant documents or records.		
Interview: Organizational personnel with continuous monitoring responsibilities.		

Table 56. CA-7(2): Continuous Monitoring

CA-7(2): Continuous Monitoring		
Control		
Plans, schedules, and conducts automated or manual assessments on a continuous and unannounced basis, of all information systems and information systems that are processing data on behalf of or directly for including, but not limited to, in-depth monitoring of systems and networks, vulnerability and configuration scanning, and announced penetration testing to ensure compliance with all vulnerability mitigation procedures.		
Guidance		
Examples of vulnerability mitigation procedures are contained in Information Assurance Vulnerability Alerts. Testing is intended to ensure that the information system continues to provide adequate security against constantly evolving threats and vulnerabilities. Conformance testing also provides independent validation. See supplemental guidance for CA-2, enhancement (2) for further information on malicious user testing, penetration testing, red-team exercises, and other forms of security testing.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.5	**Related Control Requirements:** CA-2
Assessment Procedure: CA-7(2).1		
Assessment Objective		
Determine if		
(i) the organization defines: – the forms of security testing to be included in planning, scheduling, and security control assessments selecting from in-depth monitoring, malicious user testing, penetration testing, red team exercises, or an organization-defined form of security testing to ensure compliance with all vulnerability mitigation procedures; – the frequency for conducting each form of security testing; – whether the security testing will be announced or unannounced; and (ii) the organization plans, schedules, and conducts assessments using organization-defined forms of security testing in accordance with the organization-defined frequency and assessment techniques established for		

CA-7(2): Continuous Monitoring
each form of testing to ensure compliance with all vulnerability mitigation procedures.
Assessment Methods and Objects
Examine: Security assessment and authorization policy; procedures addressing continuous monitoring of information system security controls; procedures addressing vulnerability mitigation; security plan; security assessment report; plan of action and milestones; information system monitoring records; security impact analyses; status reports; other relevant documents or records.
Interview: Organizational personnel with continuous monitoring responsibilities.

Configuration Management (CM) – Operational

Table 57. CM-1: Configuration Management Policy and Procedures

CM-1: Configuration Management Policy and Procedures		
Control		
The organization develops, disseminates, and reviews/updates within every three-hundred sixty-five (365) days: a. A formal, documented configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.		
Guidance		
This control is intended to produce the policy and procedures that are required for the effective implementation of security controls and control enhancements in the configuration management family. The configuration management policy can be included as part of the general information security policy for the organization. Configuration management procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the configuration management policy.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.6	**Related Control Requirements:**
Assessment Procedure: CM-1.1		
Assessment Objective		
Determine if:		
(i) the organization develops and formally documents configuration management policy; (ii) the organization configuration management policy addresses: – purpose; – scope; – roles and responsibilities; – management commitment; – coordination among organizational entities; – compliance; (iii) the organization disseminates formal documented configuration management policy to elements within the organization having associated configuration management roles and responsibilities; (iv) the organization develops and formally documents configuration management procedures; (v) the organization configuration management procedures facilitate implementation of the configuration management policy and associated configuration management controls; (vi) the organization disseminates formal documented configuration management procedures to elements within the organization having associated configuration management roles and responsibilities; (vii) the organization reviews/updates the configuration management policy and procedures within every three-hundred-sixty-five (365) days.		
Assessment Methods and Objects		
Examine: Configuration management policy and procedures; other relevant documents or records.		
Interview: Organizational personnel with configuration management and control responsibilities.		

Table 58. CM-2: Baseline Configuration

CM-2: Baseline Configuration		
Control		
The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.		
Guidance		
This control establishes a baseline configuration for the information system and its constituent components including communications and connectivity-related aspects of the system. The baseline configuration provides information about the components of an information system (e.g., the standard software load for a workstation, server, network component, or mobile device including operating system/installed applications with current version numbers and patch information), network topology, and the logical placement of the component within the system architecture. The baseline configuration is a documented, up-to-date specification to which the information system is built. Maintaining the baseline configuration involves creating new baselines as the information system changes over time. The baseline configuration of the information system is consistent with the organization's enterprise architecture.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.6	**Related Control Requirements:**
Assessment Procedure: CM-2.1		
Assessment Objective		
Determine if:		
(i) the organization develops and documents a baseline configuration of the information system; (ii) the organization maintains, under configuration control, a current baseline configuration of the information system. (iii) the organization documents deviations from the baseline configuration, in support of mission needs/objectives.		
Assessment Methods and Objects		
Examine: Configuration management policy; configuration management plan; procedures addressing the baseline configuration of the information system; enterprise architecture documentation; information system design documentation; information system architecture and configuration documentation; other relevant documents or records.		

Table 59. CM-2(1): System Baseline Configurations Update

CM-2(1): System Baseline Configurations Update		
Control		
The organization reviews and updates the baseline configuration of the information system: a At least once every three-hundred-sixty-five (365) days; b, When required due to major system changes/upgrades; and c, As an integral part of information system component installations and upgrades.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.6	**Related Control Requirements:**
Assessment Procedure: CM-2(1).1		
Assessment Objective		
Determine if:		
(i) the organization defines: – the frequency of reviews and updates to the baseline configuration of the information system; – the circumstances that require reviews and updates to the baseline configuration of the information system; (ii) the organization reviews and updates the baseline configuration of the information system: – in accordance with the organization-defined frequency; – when required due to organization-defined circumstances; – as an integral part of information system component installations and upgrades.		

CM-2(1): System Baseline Configurations Update
Assessment Methods and Objects
Examine: Configuration management policy; configuration management plan; procedures addressing the baseline configuration of the information system; information system architecture and configuration documentation; other relevant documents or records.
Interview: Organizational personnel with configuration change control responsibilities.

Table 60. CM-2(3): Baseline Configuration

CM-2(3): Baseline Configuration		
Control		
The organization retains older versions of baseline configurations as deemed necessary to support rollback.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.6	**Related Control Requirements:**
Assessment Procedure: CM-2(3).1		
Assessment Objective		
Determine if the organization retains older versions of baseline configurations as deemed necessary to support rollback.		
Assessment Methods and Objects		
Examine: Configuration management policy; configuration management plan; procedures addressing the baseline configuration of the information system; information system architecture and configuration documentation; historical copies of baseline configurations; other relevant documents or records.		

Table 61. CM-2(4): Software Authorized and Unauthorized Lists

CM-2(4): Software Authorized and Unauthorized Lists		
Control		
The organization: a, Develops and maintains a list of software programs authorized (white list) or unauthorized (black list) to execute on the information system; and b. Employs an allow-all, deny-by-exception authorization policy to identify software allowed to execute on the information system.		
Applicability: Exchanges	**Reference(s):**	**Related Control Requirements:**
Assessment Procedure: CM-2(4).1		
Assessment Objective		
Determine if:		
(i) the organization develops and maintains a list of software programs not authorized to execute on the information system; (ii) the organization employs an allow-all, deny-by-exception authorization policy to identify software allowed to execute on the information system.		
Assessment Methods and Objects		
Examine: Configuration management policy; configuration management plan; procedures addressing the baseline configuration of the information system; list of software programs not authorized to execute on the information system; information system architecture and configuration documentation; security plan; other relevant documents or records.		

Table 62. CM-3: Configuration Change Control

CM-3: Configuration Change Control		
Control		
The organization: a. Determines the types of changes to the information system that are configuration controlled; b. Approves configuration-controlled changes to the system with explicit consideration for security impact analyses; c. Documents approved configuration-controlled changes to the system; d. Retains and reviews records of configuration-controlled changes to the system; e. Audits activities associated with configuration-controlled changes to the system; and f. Coordinates and provides oversight for configuration change control activities through change request forms that must be approved by an organizational and/or change control board that meets frequently enough to accommodate proposed change requests, and other appropriate organization officials including, but not limited to, the System Developer/Maintainer and information system support staff.		
Guidance		
The organization determines the types of changes to the information system that are configuration controlled. Configuration change control for the information system involves the systematic proposal, justification, implementation, test/evaluation, review, and disposition of changes to the system, including upgrades and modifications. Configuration change control includes changes to components of the information system, changes to the configuration settings for information technology products (e.g., operating systems, applications, firewalls, routers), emergency changes, and changes to remediate flaws. A typical organizational process for managing configuration changes to the information system includes, for example, a chartered Configuration Control Board that approves proposed changes to the system. Auditing of changes refers to changes in activity before and after a change is made to the information system and the auditing activities required to implement the change.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.6	**Related Control Requirements:** CM-6
Assessment Procedure: CM-3.1		
Assessment Objective		
Determine if:		
(i) the organization determines the types of changes to the information system that are configuration controlled; (ii) the organization approves configuration-controlled changes to the system with explicit consideration for security impact analyses; (iii) the organization documents approved configuration-controlled changes to the system; (iv) the organization retains and reviews records of configuration-controlled changes to the system; (v) the organization audits activities associated with configuration-controlled changes to the system; (vi) the organization defines: – the configuration change control element (e.g., committee, board) responsible for coordinating and providing oversight for configuration change control activities; – the frequency with which the configuration change control element convenes, and/or; – configuration change conditions that prompt the configuration change control element to convene; (vii) the organization coordinates and provides oversight for configuration change control activities through change request forms which must be approved by an organizational and/or change control board which meets frequently enough to accommodate proposed change requests, and other appropriate organization officials including, but not limited to, the System Developer/Maintainer and information system support staff.		
Assessment Methods and Objects		
Examine: Configuration management policy; configuration management plan; procedures addressing information system configuration change control; information system architecture and configuration documentation; security plan; change control records; information system audit records; other relevant documents or records.		
Interview: Organizational personnel with configuration change control responsibilities.		

Table 63. CM-3(2): Tests, Validates, and Documents Changes

CM-3(2): Tests, Validates, and Documents Changes		
Control		
The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.		
Guidance		
The organization ensures that testing does not interfere with information system operations. The individual/group conducting the tests understands the information security policies and procedures, the information system security policies and procedures, and the specific health, safety, and environmental risks associated with a particular facility and/or process. An operational system may need to be taken off-line, or replicated to the extent feasible, before testing can be conducted. If an information system must be taken off-line for testing, the tests are scheduled to occur during planned system outages whenever possible. In situations where the organization cannot conduct testing of an operational system, the organization employs compensating controls (e.g., providing a replicated system to conduct testing) in accordance with the general tailoring guidance.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.6	**Related Control Requirements:**
Assessment Procedure: CM-3(2).1		
Assessment Objective		
Determine if the organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.		
Assessment Methods and Objects		
Examine: Configuration management policy; configuration management plan; procedures addressing information system configuration change control; information system design documentation; information system architecture and configuration documentation; change control records; information system audit records; other relevant documents or records.		
Interview: Organizational personnel with configuration change control responsibilities.		

Table 64. CM-4: Security Impact Analysis

CM-4: Security Impact Analysis		
Control		
The organization analyzes changes to the information system to determine potential security impacts prior to change implementation. Activities associated with configuration changes to the information system are audited.		
Guidance		
Security impact analyses are conducted by organizational personnel with information security responsibilities, including, for example, Information System Administrators, Information System Security Officers, Information System Security Managers, and Information System Security Engineers. Individuals conducting security impact analyses have the appropriate skills and technical expertise to analyze the changes to information systems and the associated security ramifications. Security impact analysis may include, for example, reviewing information system documentation such as the security plan to understand how specific security controls are implemented within the system and how the changes might affect the controls. Security impact analysis may also include an assessment of risk to understand the impact of the changes and to determine if additional security controls are required. Security impact analysis is scaled in accordance with the impact level of the information system.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.6	**Related Control Requirements:** CA-2, CA-7, CM-3, CM-9, SI-2
Assessment Procedure: CM-4.1		
Assessment Objective		
Determine if the organization analyzes changes to the information system to determine potential security impacts prior to change implementation.		

CM-4: Security Impact Analysis
Assessment Methods and Objects
Examine: Configuration management policy; configuration management plan; procedures addressing security impact analysis for changes to the information system; security impact analysis documentation; information system architecture and configuration documentation; change control records; information system audit records; other relevant documents or records.
Interview: Organizational personnel with responsibilities for determining security impacts prior to implementation of information system changes.

Table 65. CM-4(1): Security Impact Analysis

CM-4(1): Security Impact Analysis		
Control		
The organization analyzes new software in a separate test environment before installation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.		
Guidance		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.6	**Related Control Requirements:**
Assessment Procedure: CM-4(1).1		
Assessment Objective		
Determine if:		
(i) the organization analyzes new software in a separate test environment before installation in an operational environment; and (ii) the organization, when analyzing new software in a separate test environment, looks for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.		
Assessment Methods and Objects		
Examine: Configuration management policy; configuration management plan; procedures addressing security impact analysis for changes to the information system; security impact analysis documentation; information system design documentation; information system architecture and configuration documentation; change control records; information system audit records; information system test and operational environments; other relevant documents or records.		
Interview: Organizational personnel with responsibilities for determining security impacts prior to implementation of information system changes.		

Table 66. CM-4(2): Security Impact Analysis

CM-4(2): Security Impact Analysis		
Control		
The organization, after the information system is changed, checks the security functions to verify that the functions are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security requirements for the system.		
Guidance		
Changes include information system upgrades and modifications.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.6	**Related Control Requirements:**
Assessment Procedure: CM-4(2).1		
Assessment Objective		
Determine if the organization, after the information system is changed, checks the security functions to verify that the		

CM-4(2): Security Impact Analysis
functions are: (i) implemented correctly; (ii) operating as intended; and (iii) producing the desired outcome with regard to meeting the security requirements for the system.
Assessment Methods and Objects
Examine: Configuration management policy; configuration management plan; procedures addressing security impact analysis for changes to the information system; security impact analysis documentation; change control records; information system audit records; other relevant documents or records.
Interview: Organizational personnel with responsibilities for determining security impacts prior to implementation of information system changes.

Table 67. CM-5: Access Restrictions for Change

CM-5: Access Restrictions for Change		
Control		
The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system. Records reflecting all such changes shall be generated, reviewed, and retained.		
Guidance		
Any changes to the hardware, software, and/or firmware components of the information system can potentially have significant effects on the overall security of the system. Accordingly, only qualified and authorized individuals are allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications. Additionally, maintaining records of access is essential for ensuring that configuration change control is being implemented as intended and for supporting after-the-fact actions should the organization become aware of an unauthorized change to the information system. Access restrictions for change also include software libraries. Examples of 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 are implemented into a third-party interface rather than directly into the information system component), and change windows (e.g., changes occur only during specified times, making unauthorized changes outside the window easy to discover). Some or all of the enforcement mechanisms and processes necessary to implement this security control are included in other controls. For measures implemented in other controls, this control provides information to be used in the implementation of the other controls to cover specific needs related to enforcing authorizations to make changes to the information system, auditing changes, and retaining and review records of changes.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.6	**Related Control Requirements:**
Assessment Procedure: CM-5.1		
Assessment Objective		
Determine if:		
(i) the organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system. (ii) the organization generates, reviews, and retains records reflecting all such changes.		
Assessment Methods and Objects		
Examine: Configuration management policy; configuration management plan; procedures addressing access restrictions for changes to the information system; information system architecture and configuration documentation; change control records; information system audit records; other relevant documents or records.		
Interview: Organizational personnel with logical access control responsibilities; organizational personnel with physical access control responsibilities.		

Table 68. CM-6: Configuration Settings

CM-6: Configuration Settings

Control

The organization:

a. Establishes and documents mandatory configuration settings for information technology products employed within the information system using the latest security configuration guidelines listed in Implementation Standard 1 that reflect the most restrictive mode consistent with operational requirements;
b. Implements the configuration settings;
c. Identifies, documents, and approves exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements; and
d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

For FTI: Establish mandatory configuration settings for systems that receive, store, process and transmit FTI using the Safeguards Computer Security Evaluation Matrices (SCSEMs).

Implementation Standards

1. Security configuration guidelines may be developed by different federal agencies, so it is possible that a guideline could include configuration information that conflicts with another agency or the organization's guideline. To resolve configuration conflicts among multiple security guidelines, the organization's hierarchy for implementing all security configuration guidelines is as follows:
   – NIST
   – CMS
   – DISA
   – OMB

For FTI: SCSEMs – All agency information systems used for receiving, processing, storing and transmitting FTI must be hardened in accordance with the requirements of Publication 1075. Agency information systems include the equipment, facilities, and people that collect, process, store, display and disseminate information. This includes computers, hardware, software, and communications, as well as policies and procedures for their use. Safeguard Computer Security Evaluation Matrices (SCSEMs) provide hardening guidance for specific technologies and are publicly available on the Office of Safeguards IRS.gov website, keyword: safeguards program.

Guidance

Configuration settings are the configurable security-related parameters of information technology products that are part of the information system. Security-related parameters are those parameters impacting the security state of the system including parameters related to meeting other security control requirements. Security-related parameters include, for example, registry settings; account, file, and directory settings (i.e., permissions); and settings for services, ports, protocols, and remote connections. Organizations establish organization-wide mandatory configuration settings from which the settings for a given information system are derived. A security configuration checklist [sometimes referred to as a lockdown guide, hardening guide, security guide, security technical implementation guide (STIG), or benchmark] is a series of instructions or procedures for configuring an information system component to meet operational requirements. Checklists can be developed by information technology developers and vendors, consortia, academia, industry, federal agencies (and other government organizations), and others in the public and private sectors. An example of a security configuration checklist is the Federal Desktop Core Configuration (FDCC), which potentially affects the implementation of CM-6 and other controls such as AC-19 and CM-7. The Security Content Automation Protocol (SCAP) and defined standards within the protocol (e.g., Common Configuration Enumeration) provide an effective method to uniquely identify, track, and control configuration settings.

Applicability: Exchanges	**Reference(s):** CM-3, CM-8, SI-4; IRS-1075: 9.6	**Related Control Requirements:** CM-3, CM-8, SI-4

Assessment Procedure: CM-6.1

CM-6: Configuration Settings
Assessment Objective
Determine if:
(i) the organization defines security configuration checklists to be used to establish and document mandatory configuration settings for the information system technology products employed; (ii) the organization-defined security configuration checklists reflect the most restrictive mode consistent with operational requirements; (iii) the organization establishes and documents mandatory configuration settings for information technology products employed within the information system using organization-defined security configuration checklists; (iv) the organization implements the security configuration settings; (v) the organization identifies, documents, and approves exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements; (vi) the organization monitors and controls changes to the configuration settings in accordance with organizational policies and procedures. (vii) the organization meets all the requirements specified in the applicable implementation standard(s).
Assessment Methods and Objects
Examine: Configuration management policy; configuration management plan; procedures addressing configuration settings for the information system; security plan; information system configuration settings and associated documentation; security configuration checklists; other relevant documents or records.
Interview: Organizational personnel with security configuration responsibilities.

Table 69. CM-6(3): Detects Unauthorized Configuration Changes

CM-6(3): Detects Unauthorized Configuration Changes		
Control		
The organization incorporates detection of unauthorized, security-relevant configuration changes into the organization's incident response capability to ensure that such detected events are tracked, monitored, corrected, and available for historical purposes.		
Applicability: Exchanges	**Reference(s):**	**Related Control Requirements:**
Assessment Procedure: CM-6(3).1		
Assessment Objective		
Determine if:		
(i) the organization incorporates detection of unauthorized, security-relevant configuration changes into the organization's incident response capability; (ii) the organization ensures that such detected events are tracked, monitored, corrected, and available for historical purposes.		
Assessment Methods and Objects		
Examine: Configuration management policy; configuration management plan; procedures addressing configuration settings for the information system; procedures addressing incident response planning; information system design documentation; information system configuration settings and associated documentation; incident response plan; other relevant documents or records.		
Interview: Organizational personnel with security configuration responsibilities; organization personnel with incident response planning responsibilities.		

Table 70. CM-7: Least Functionality

<table>
<tr><th colspan="3">CM-7: Least Functionality</th></tr>
<tr><td colspan="3"><b>Control</b></td></tr>
<tr><td colspan="3">The organization configures the information system to provide only essential capabilities and specifically disables, prohibits, or restricts the use of system services, ports, network protocols, and capabilities that are not explicitly required for system or application functionality. A list of specifically needed system services, ports, and network protocols will be maintained and documented in the SSP; all others will be disabled.</td></tr>
<tr><td colspan="3"><b>Guidance</b></td></tr>
<tr><td colspan="3">Information systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential operations (e.g., key missions, functions). Additionally, it is sometimes convenient to provide multiple services from a single component of an information system, 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 server or web server, not both). The functions and services provided by the organization's information systems, or individual components of information systems, are carefully reviewed to determine which functions and services are candidates for elimination (e.g., Voice Over Internet Protocol, Instant Messaging, auto-execute, file sharing). Organizations consider disabling unused or unnecessary physical and logical ports and protocols (e.g., Universal Serial Bus [USB], File Transfer Protocol [FTP], Internet Protocol Version 6 [IPv6], Hyper Text Transfer Protocol [HTTP]) on information system components 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.</td></tr>
<tr><td><b>Applicability:</b> Exchanges</td><td><b>Reference(s):</b> IRS-1075: 9.6</td><td><b>Related Control Requirements:</b></td></tr>
<tr><td colspan="3"><b>Assessment Procedure: CM-7.1</b></td></tr>
<tr><td colspan="3"><b>Assessment Objective</b></td></tr>
<tr><td colspan="3">Determine if:</td></tr>
<tr><td colspan="3">(i) the organization defines for the information system prohibited or restricted:
– functions;
– ports;
– protocols;
– services;
(ii) the organization configures the information system to provide only essential capabilities;
(iii) the organization configures the information system to specifically prohibit or restrict the use of organization-defined:
– functions;
– ports;
– protocols; and/or
– services</td></tr>
<tr><td colspan="3"><b>Assessment Methods and Objects</b></td></tr>
<tr><td colspan="3"><b>Examine:</b> Configuration management policy; configuration management plan; procedures addressing least functionality in the information system; security plan; information system configuration settings and associated documentation; security configuration checklists; other relevant documents or records.</td></tr>
</table>

Table 71. CM-7(1): Least Functionality Review

<table>
<tr><th colspan="3">CM-7(1): Least Functionality Review</th></tr>
<tr><td colspan="3"><b>Control</b></td></tr>
<tr><td colspan="3">The organization reviews the information system within every three-hundred-sixty-five (365) days to identify and eliminate unnecessary functions, ports, protocols, and/or services.</td></tr>
<tr><td><b>Applicability:</b> Exchanges</td><td><b>Reference(s):</b></td><td><b>Related Control Requirements:</b></td></tr>
</table>

CM-7(1): Least Functionality Review
Assessment Procedure: CM-7(1).1
Assessment Objective
Determine if:

(i) the organization defines the frequency of information system reviews to identify and eliminate unnecessary:
– functions;
– ports;
– protocols; and/or
– services;
(ii) the organization reviews the information system in accordance with organization defined frequency to identify and eliminate unnecessary:
– functions;
– ports;
– protocols; and/or
– services.

Assessment Methods and Objects
Examine: Configuration management policy; configuration management plan; procedures addressing least functionality in the information system; security plan; information system configuration settings and associated documentation; security configuration checklists; other relevant documents or records.
Interview: Organizational personnel with responsibilities for identifying and eliminating unnecessary functions, ports, protocols, and services on the information system.

Table 72. CM-8: Information System Component Inventory

<table>
<tr><th colspan="3">CM-8: Information System Component Inventory</th></tr>
<tr><td colspan="3"><b>Control</b></td></tr>
<tr><td colspan="3">The organization develops, documents, and maintains an inventory of information system components that:
a. Accurately reflects the current information system;
b. Is consistent with the authorization boundary of the information system;
c. Is at the level of granularity deemed necessary for tracking and reporting;
d. Includes manufacturer, model/type, serial number, version number, location (i.e., physical location and logical position within the information system architecture), and ownership; and
e. Is available for review and audit by designated organizational officials.</td></tr>
<tr><td colspan="3"><b>Guidance</b></td></tr>
<tr><td colspan="3">Information deemed to be necessary by the organization to achieve effective property accountability can include, for example, hardware inventory specifications (manufacturer, type, model, serial number, physical location), software license information, information system/component owner, and for a networked component/device, the machine name and network address.</td></tr>
<tr><td><b>Applicability:</b> Exchanges</td><td><b>Reference(s):</b> HIPAA: 164.310(d)(1), 164.310(d)(2)(iii); IRS-1075: 9.6</td><td><b>Related Control Requirements:</b> CM-6</td></tr>
<tr><td colspan="3"><b>Assessment Procedure: CM-8.1</b></td></tr>
<tr><td colspan="3"><b>Assessment Objective</b></td></tr>
<tr><td colspan="3">Determine if:</td></tr>
<tr><td colspan="3">(i) the organization defines information deemed necessary to achieve effective property accountability;
(ii) the organization develops, documents, and maintains an inventory of information system components that:
– accurately reflects the current information system;
– is consistent with the authorization boundary of the information system;
– is at the level of granularity deemed necessary for tracking and reporting;
– includes organization-defined information deemed necessary to achieve effective property accountability;
– is available for review and audit by designated organizational officials.</td></tr>
<tr><td colspan="3"><b>Assessment Methods and Objects</b></td></tr>
</table>

<table>
<tr><th>CM-8: Information System Component Inventory</th></tr>
<tr><td><b>Examine:</b> Configuration management policy; configuration management plan; procedures addressing information system component inventory; security plan; information system inventory records; other relevant documents or records.</td></tr>
</table>

Table 73. CM-8(1): System Component Inventory Update

<table>
<tr><th colspan="3">CM-8(1): System Component Inventory Update</th></tr>
<tr><td colspan="3"><b>Control</b></td></tr>
<tr><td colspan="3">The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.</td></tr>
<tr><td><b>Applicability:</b> Exchanges</td><td><b>Reference(s):</b> HIPAA: 164.310(d)(1), 164.310(d)(2)(iii); IRS-1075: 9.6</td><td><b>Related Control Requirements:</b></td></tr>
<tr><td colspan="3"><b>Assessment Procedure: CM-8(1).1</b></td></tr>
<tr><td colspan="3"><b>Assessment Objective</b></td></tr>
<tr><td colspan="3">Determine if the organization updates the inventory of information system components as an integral part of component:
(iii) installations;
(i) removals;
(ii) information system updates.</td></tr>
<tr><td colspan="3"><b>Assessment Methods and Objects</b></td></tr>
<tr><td colspan="3"><b>Examine:</b> Configuration management policy; configuration management plan; procedures addressing information system component inventory; information system inventory records; component installation records; other relevant documents or records.</td></tr>
<tr><td colspan="3"><b>Interview:</b> Organizational personnel with information system installation and inventory responsibilities.</td></tr>
</table>

Table 74. CM-9: Configuration Management Plan

<table>
<tr><th colspan="3">CM-9: Configuration Management Plan</th></tr>
<tr><td colspan="3"><b>Control</b></td></tr>
<tr><td colspan="3">The organization develops, documents, and implements a configuration management plan for the information system that:
a. Addresses roles, responsibilities, and configuration management processes and procedures;
b. Defines the configuration items for the information system and when in the system development life cycle the configuration items are placed under configuration management; and
c. Establishes the means for identifying configuration items throughout the system development life cycle and a process for managing the configuration of the configuration items.</td></tr>
<tr><td colspan="3"><b>Guidance</b></td></tr>
<tr><td colspan="3">Configuration items are the information system items (hardware, software, firmware, and documentation) to be configuration managed. The configuration management plan satisfies the requirements in the organization’s configuration management policy while being tailored to the individual information system. The configuration management plan defines detailed processes and procedures for how configuration management is used to support system development life cycle activities at the information system level. The plan describes how to move a change through the change management process, how configuration settings and configuration baselines are updated, how the information system component inventory is maintained, how development, test, and operational environments are controlled, and finally, how documents are developed, released, and updated. The configuration management approval process includes designation of key management stakeholders that are responsible for reviewing and approving proposed changes to the information system, and security personnel that would conduct an impact analysis prior to the implementation of any changes to the system.</td></tr>
<tr><td><b>Applicability:</b> Exchanges</td><td><b>Reference(s):</b> IRS-1075: 9.6</td><td><b>Related Control Requirements:</b></td></tr>
<tr><td colspan="3"><b>Assessment Procedure: CM-9.1</b></td></tr>
</table>

CM-9: Configuration Management Plan
Assessment Objective
Determine if the organization develops, documents, and implements a configuration management plan for the information system that: (i) addresses roles, responsibilities, and configuration management processes and procedures; (ii) defines the configuration items for the information system and when in the system development life cycle the configuration items are placed under configuration management; (iii) establishes the means for identifying configuration items throughout the system development life cycle and a process for managing the configuration of the configuration items.
Assessment Methods and Objects
Examine: Configuration management policy; configuration management plan; procedures addressing configuration management planning; security plan; other relevant documents or records.

Contingency Planning (CP) – Operational

Table 75. CP-1: Contingency Planning Policy and Procedures

CP-1: Contingency Planning Policy and Procedures		
Control		
The organization develops, disseminates, and reviews/updates within every three-hundred-sixty-five (365) days: a. A formal, documented contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.		
Guidance		
This control is intended to produce the policy and procedures that are required for the effective implementation of security controls and control enhancements in the contingency planning family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The contingency planning policy can be included as part of the general information security policy for the organization. Contingency planning procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the contingency planning policy.		
Applicability: Exchanges	**Reference(s):** HIPAA: 164.308(a)(7)(i), 164.308(a)(7)(ii)(B); IRS-1075: 9.7	**Related Control Requirements:**
Assessment Procedure: CP-1.1		
Assessment Objective		
Determine if:		
(i) the organization develops and formally documents contingency planning policy; (ii) the organization contingency planning policy addresses: – purpose; – scope; – roles and responsibilities; – management commitment; – coordination among organizational entities; – compliance; (iii) the organization disseminates formal documented contingency planning policy to elements within the organization having associated contingency planning roles and responsibilities; (iv) the organization develops and formally documents contingency planning procedures; (v) the organization contingency planning procedures facilitate implementation of the contingency planning policy and associated contingency planning controls; (vi) the organization disseminates formal documented contingency planning procedures to elements within the organization having associated contingency planning roles and responsibilities; (vii) the organization reviews/updates the contingency planning policy and procedures within every three-hundred-sixty-five (365) days.		
Assessment Methods and Objects		
Examine: Contingency planning policy and procedures; other relevant documents or records.		
Interview: Organizational personnel with contingency planning responsibilities.		

Table 76. CP-2: Contingency Plan

CP-2: Contingency Plan

Control

The organization:

a. Develops a Contingency Plan (CP) for the information system that:
   - – Identifies essential Exchange missions and business functions and associated contingency requirements;
   - – Provides recovery objectives, restoration priorities, and metrics;
   - – Addresses contingency roles, responsibilities, assigned individuals with contact information;
   - – Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;
   - – Addresses eventual, full information system restoration without deterioration of the security measures originally planned and implemented; and
   - – Is reviewed and approved by designated officials within the organization;

b. Distributes copies of the CP plan to 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 CP for the information system within every three-hundred-sixty-five (365) days;

e. Revises the CP to address changes to the organization, information system, or environment of operation and problems encountered during CP implementation, execution, or testing; and

f. Communicates CP changes to key contingency personnel (identified by name and/or by role) and organizational elements.

Guidance

Contingency planning for information systems is part of an overall organizational program for achieving continuity of operations for the organization's mission/business operations. Contingency planning addresses both information system restoration and implementation of alternative mission/business processes when systems are compromised. Information system recovery objectives are consistent with applicable laws, Executive Orders, directives, policies, standards, or regulations. In addition to information system availability, contingency plans also address other security-related events resulting in a reduction in mission/business effectiveness, such as malicious attacks compromising the confidentiality or integrity of the information system. Examples of actions to call out in contingency plans include, for example, graceful degradation, information system shutdown, fall back to a manual mode, alternate information flows, or operating in a mode that is reserved solely for when the system is under attack. Copies of the current CP are stored in a secure location at an alternate site accessible by management and other key personnel.

Applicability: Exchanges	**Reference(s):** HIPAA: 164.308(a)(7)(ii)(E), 164.312(a)(2)(ii); HSPD 7: G(22)(i); IRS-1075: 9.7	**Related Control Requirements:**

Assessment Procedure: CP-2.1

Assessment Objective

Determine if:

(i) the organization develops a contingency plan for the information system that:
   - – identifies essential missions and business functions and associated contingency requirements;
   - – provides recovery objectives, restoration priorities, and metrics;
   - – addresses contingency roles, responsibilities, assigned individuals with contact information;
   - – addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;
   - – addresses eventual, full information system restoration without deterioration of the security measures originally planned and implemented;
   - – is reviewed and approved by designated officials within the organization;

(ii) the organization defines key contingency personnel (identified by name and/or by role) and organizational elements designated to receive copies of the contingency plan;

(iii) the organization distributes copies of the contingency plan to organization-defined key contingency personnel and organizational elements.

CP-2: Contingency Plan
Assessment Methods and Objects
Examine: Contingency planning policy; procedures addressing contingency operations for the information system; contingency plan; security plan; other relevant documents or records.
Interview: Organizational personnel with contingency planning and plan implementation responsibilities
Assessment Procedure: CP-2.2
Assessment Objective:
Determine if:
(i) the organization coordinates contingency planning activities with incident handling activities; (ii) the organization defines the frequency of contingency plan reviews; (iii) the organization reviews the contingency plan for the information system in accordance with the organization-defined frequency; (iv) the organization revises 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; (v) the organization communicates contingency plan changes to the key contingency personnel and organizational elements.
Assessment Methods And Objects
Examine: Contingency planning policy; procedures addressing contingency operations for the information system; contingency plan; security plan; other relevant documents or records.
Interview: Organizational personnel with contingency planning and plan implementation responsibilities; organizational personnel with incident handling responsibilities.

Table 77. CP-2(1): Contingency Plan

CP-2(1): Contingency Plan		
Control		
The organization coordinates contingency plan development with organizational elements responsible for related plans. Enhancement Supplemental Guidance: Examples of related plans include Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Crisis Communications Plan, Critical Infrastructure Plan, Cyber Incident Response Plan, and Occupant Emergency Plan.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.7	**Related Control Requirements:**
Assessment Procedure: CP-2(1).1		
Assessment Objective		
Determine if the organization coordinates the contingency plan development with other organizational elements responsible for related plans.		
Assessment Methods and Objects		
Examine: Contingency planning policy; procedures addressing contingency operations for the information system; contingency plan; other related plans; other relevant documents or records.		
Interview: Organizational personnel with contingency planning and plan implementation responsibilities and responsibilities in related plan areas.		

Table 78. CP-2(2): Contingency Plan

CP-2(2): Contingency Plan		
Control		
The organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.7	**Related Control Requirements:**
Assessment Procedure: CP-2(2).1		
Assessment Objective		
Determine if the organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.		
Assessment Methods and Objects		
Examine: Contingency planning policy; procedures addressing contingency operations for the information system; contingency plan; capacity planning documents; other relevant documents or records.		
Interview: Organizational personnel with contingency planning and plan implementation responsibilities.		

Table 79. CP-3: Contingency Training

CP-3: Contingency Training		
Control		
The organization trains operational and support personnel (including managers and users of the information system) in their contingency roles and responsibilities with respect to the information system and provides refresher training within every three hundred sixty-five (365) days.		
Guidance		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.7	**Related Control Requirements:**
Assessment Procedure: CP-3.1		
Assessment Objective		
Determine if:		
(i) the organization provides initial contingency training to personnel with contingency roles and responsibilities with respect to the information system; (ii) the organization defines the frequency of refresher contingency training; and (iii) the organization provides refresher training in accordance with organization-defined frequency.		
Assessment Methods and Objects		
Examine: Contingency planning policy; contingency plan; procedures addressing contingency training; contingency training curriculum; contingency training material; security plan; contingency training records; other relevant documents or records.		
Interview: Organizational personnel with contingency planning, plan implementation, and training responsibilities.		

Table 80. CP-4: Contingency Plan Testing and Exercises

CP-4: Contingency Plan Testing and Exercises		
Control		
The organization trains operational and support personnel (including managers and users of the information system) in their contingency roles and responsibilities with respect to the information system and provides refresher training within every three hundred sixty-five (365) days.		
Guidance		
There are several methods for testing and/or exercising contingency plans to identify potential weaknesses (e.g., checklist, walk-through/tabletop, simulation: parallel, full interrupt). Contingency plan testing and/or exercises include a determination of the effects on organizational operations and assets (e.g., reduction in mission capability) and individuals arising due to contingency operations in accordance with the plan.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.7	**Related Control Requirements:**
Assessment Procedure: CP-4.1		
Assessment Objective		
Determine if:		
(i) the organization defines the contingency plan tests and/or exercises to be conducted; (ii) the organization defines the frequency of contingency plan tests and/or exercises; (iii) the organization tests/exercises the contingency plan using organization-defined tests/exercises in accordance with organization-defined frequency; and (iv) the organization reviews the contingency plan test/exercise results and takes corrective actions.		
Assessment Methods and Objects		
Examine: Contingency planning policy; contingency plan, procedures addressing contingency plan testing and exercises; security plan; contingency plan testing and/or exercise documentation; other relevant documents or records.		
Interview: Organizational personnel with responsibilities for reviewing or responding to contingency plan tests/exercises.		

Table 81. CP-4(1): Contingency Plan Testing and Exercises

CP-4(1): Contingency Plan Testing and Exercises		
Control		
The organization coordinates contingency plan testing and/or exercises with organizational elements responsible for related plans.		
Guidance		
Examples of related plans include Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Crisis Communications Plan, Critical Infrastructure Plan, Cyber Incident Response Plan, and Occupant Emergency Plan.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.7	**Related Control Requirements:**
Assessment Procedure: CP-4(1).1		
Assessment Objective		
Determine if the organization coordinates contingency plan testing and/or exercises with organizational elements responsible for related plans.		
Assessment Methods and Objects		
Examine: Contingency planning policy; contingency plan; procedures addressing contingency plan testing and exercises; contingency plan testing and/or exercise documentation; other relevant documents or records.		
Interview: Organizational personnel with contingency planning, plan implementation, and testing responsibilities; organizational personnel with responsibilities for related plans.		

Table 82. CP-6: Alternate Storage Site

CP-6: Alternate Storage Site		
Control		
The organization establishes an alternate storage site including necessary agreements to permit the storage and recovery of information system backup information. For FTI: The agency must identify alternative storage sites and initiate necessary agreements to permit the secure storage of information system and FTI backups and ensure the alternative storage sites meet FTI secure storage requirements.		
Guidance		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.7	**Related Control Requirements:** CP-2, CP-9, MP-4
Assessment Procedure: CP-6.1		
Assessment Objective		
Determine if:		
(i) the organization establishes an alternate storage site; and (ii) the organization initiates necessary alternate storage site agreements to permit the storage and recovery of information system backup information.		
Assessment Methods and Objects		
Examine: Contingency planning policy; contingency plan; procedures addressing alternate storage sites; alternate storage site agreements; other relevant documents or records.		

Table 83. CP-6(1): Alternate Storage Site

CP-6(1): Alternate Storage Site		
Control		
The organization identifies an alternate storage site that is separated from the primary storage site so as not to be susceptible to the same hazards.		
Guidance		
Hazards of concern to the organization are typically defined in an organizational assessment of risk.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.7	**Related Control Requirements:**
Assessment Procedure: CP-6(1).1		
Assessment Objective		
Determine if:		
(i) the contingency plan identifies the primary storage site hazards; and (ii) the alternate storage site is separated from the primary storage site so as not to be susceptible to the same hazards identified at the primary site.		
Assessment Methods and Objects		
Examine: Contingency planning policy; contingency plan; procedures addressing alternate storage sites; alternate storage site; other relevant documents or records.		

Table 84. CP-6(3): Alternate Storage Site

CP-6(3): Alternate Storage Site		
Control		
The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.		
Guidance		
Explicit mitigation actions include, for example, duplicating backup information at another alternate storage site if access to the first alternate site is hindered; or, if electronic accessibility to the alternate site is disrupted, planning for physical access to retrieve backup information.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.7	**Related Control Requirements:**
Assessment Procedure: CP-6(3).1		
Assessment Objective		
Determine if:		
(i) the organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster; and (ii) the organization outlines explicit mitigation actions for organization identified accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster.		
Assessment Methods and Objects		
Examine: Contingency planning policy; contingency plan; procedures addressing alternate storage sites; alternate storage site; mitigation actions for accessibility problems to the alternate storage site; other relevant documents or records.		

Table 85. CP-7: Alternate Processing Site

CP-7: Alternate Processing Site		
Control		
The organization: a. Establishes an alternate processing site including necessary agreements to permit the resumption of information system operations for essential missions and business functions within the time period specified in Implementation Standard 1 when the primary processing capabilities are unavailable; and b. Ensures that equipment and supplies required to resume operations are available at the alternate site or contracts are in place to support delivery to the site in time to support the time period for resumption specified in Implementation Standard 1.		
Implementation Standard		
1. Ensure all equipment and supplies required for resuming system operations at the alternate processing site are available, or contracts are in place to support delivery to the site, to permit resumption of essential missions and business functions within one (1) week of contingency plan activation.		
Guidance		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.7	**Related Control Requirements:** CP-2

CP-7: Alternate Processing Site
Assessment Procedure: CP-7.1
Assessment Objective
Determine if:
(i) the organization establishes an alternate processing site; (ii) the organization defines the time period for achieving the recovery time objectives within which processing must be resumed at the alternate processing site; (iii) the organization includes necessary alternate processing site agreements to permit the resumption of information system operations for essential missions and business functions within organization-defined time period; and (iv) the equipment and supplies required to resume operations are available at the alternate site or contracts are in place to support delivery to the site in time to support the organization-defined time period for resumption.
Assessment Methods and Objects
Examine: Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site agreements; security plan; spare equipment and supplies at alternate processing site; equipment and supply contracts; service level agreements; other relevant documents or records.

Table 86. CP-7(1): Alternate Processing Site

CP-7(1): Alternate Processing Site		
Control		
The organization identifies an alternate processing site that is separated from the primary processing site so as not to be susceptible to the same hazards.		
Guidance		
Hazards that might affect the information system are typically defined in the risk assessment.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.7	**Related Control Requirements:**
Assessment Procedure: CP-7(1).1		
Assessment Objective		
Determine if:		
(i) the contingency plan identifies the primary processing site hazards; and (ii) the alternate processing site is separated from the primary processing site so as not to be susceptible to the same hazards identified at the primary site.		
Assessment Methods and Objects		
Examine: Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site; other relevant documents or records.		

Table 87. CP-7(2): Alternate Processing Site

CP-7(2): Alternate Processing Site		
Control		
The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.		
Guidance		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.7	**Related Control Requirements:**
Assessment Procedure: CP-7(2).1		

CP-7(2): Alternate Processing Site
Assessment Objective
Determine if:
(i) the organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster; and (ii) the organization outlines explicit mitigation actions for organization identified accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster.
Assessment Methods and Objects
Examine: Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site; other relevant documents or records.

Table 88. CP-7(3): Alternate Processing Site

<table>
<tr><th colspan="3">CP-7(3): Alternate Processing Site</th></tr>
<tr><td colspan="3"><b>Control</b></td></tr>
<tr><td colspan="3">The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with the organization's availability requirements.</td></tr>
<tr><td colspan="3"><b>Guidance</b></td></tr>
<tr><td colspan="3"></td></tr>
<tr><td><b>Applicability:</b> Exchanges</td><td><b>Reference(s):</b> IRS-1075: 9.7</td><td><b>Related Control Requirements:</b></td></tr>
<tr><td colspan="3"><b>Assessment Procedure: CP-7(3).1</b></td></tr>
<tr><td colspan="3"><b>Assessment Objective</b></td></tr>
<tr><td colspan="3">Determine if the organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with the organization’s availability requirements.</td></tr>
<tr><td colspan="3"><b>Assessment Methods and Objects</b></td></tr>
<tr><td colspan="3"><b>Examine:</b> Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site agreements; other relevant documents or records.</td></tr>
</table>

Table 89. CP-7(5): Alternate Processing Site

<table>
<tr><th colspan="3">CP-7(5): Alternate Processing Site</th></tr>
<tr><td colspan="3"><b>Control</b></td></tr>
<tr><td colspan="3">The organization ensures that the alternate processing site provides information security measures equivalent to that of the primary site.</td></tr>
<tr><td colspan="3"><b>Guidance</b></td></tr>
<tr><td colspan="3"></td></tr>
<tr><td><b>Applicability:</b> Exchanges</td><td><b>Reference(s):</b> IRS-1075: 9.7</td><td><b>Related Control Requirements:</b></td></tr>
<tr><td colspan="3"><b>Assessment Procedure: CP-7(5).1</b></td></tr>
<tr><td colspan="3"><b>Assessment Objective</b></td></tr>
<tr><td colspan="3">Determine if the alternate processing site provides information security measures equivalent to that of the primary site.</td></tr>
<tr><td colspan="3"><b>Assessment Methods and Objects</b></td></tr>
<tr><td colspan="3"><b>Examine:</b> Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site; other relevant documents or records.</td></tr>
</table>

Table 90. CP-8: Telecommunications Services

<table>
<tr><th colspan="3">CP-8: Telecommunications Services</th></tr>
<tr><td colspan="3"><b>Control</b></td></tr>
<tr><td colspan="3">The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of information system operations for essential missions and business functions within the resumption time period specified in Implementation Standard 1 when the primary telecommunications capabilities are unavailable.</td></tr>
<tr><td colspan="3"><b>Implementation Standard</b></td></tr>
<tr><td colspan="3">1. Ensure alternate telecommunications service agreements are in place to permit resumption of information system operations for essential missions and business functions within one (1) week of contingency plan activation when primary telecommunications capabilities are unavailable.</td></tr>
<tr><td colspan="3"><b>Guidance</b></td></tr>
<tr><td colspan="3"></td></tr>
<tr><td><b>Applicability:</b> Exchanges</td><td><b>Reference(s):</b></td><td><b>Related Control Requirements:</b> CP-2</td></tr>
<tr><td colspan="3"><b>Assessment Procedure: CP-8.1</b></td></tr>
<tr><td colspan="3"><b>Assessment Objective</b></td></tr>
<tr><td colspan="3">Determine if:</td></tr>
<tr><td colspan="3">(i) the organization establishes alternate telecommunications services to support the information system;
(ii) the organization defines in the time period within which resumption of information system operations must take place; and
(iii) the organization establishes necessary alternate telecommunications service agreements to permit the resumption of telecommunications services for essential missions and business functions within the organization-defined time period when the primary telecommunications capabilities are unavailable.</td></tr>
<tr><td colspan="3"><b>Assessment Methods and Objects</b></td></tr>
<tr><td colspan="3"><b>Examine:</b> Contingency planning policy; contingency plan; procedures addressing alternate telecommunications services; security plan; primary and alternate telecommunications service agreements; list of essential missions and business functions; other relevant documents or records<b>.</b></td></tr>
</table>

Table 91. CP-8(1): Telecommunication Services

<table>
<tr><th colspan="3">CP-8(1): Telecommunications Services</th></tr>
<tr><td colspan="3"><b>Control</b></td></tr>
<tr><td colspan="3">The organization:
a. develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with the organization's availability requirements; and
b. Requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier.</td></tr>
<tr><td colspan="3"><b>Guidance</b></td></tr>
<tr><td colspan="3"></td></tr>
<tr><td><b>Applicability:</b> Exchanges</td><td><b>Reference(s):</b></td><td><b>Related Control Requirements:</b></td></tr>
<tr><td colspan="3"><b>Assessment Procedure: CP-8(1).1</b></td></tr>
<tr><td colspan="3"><b>Assessment Objective</b></td></tr>
</table>

CP-8(1): Telecommunications Services
Determine if:
(i) the organization develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with organizational availability requirements; and (ii) the organization requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier.
Assessment Methods and Objects
Examine: Contingency planning policy; contingency plan; procedures addressing alternate telecommunications services; primary and alternate telecommunications service agreements; Telecommunications Service Priority documentation; other relevant documents or records.

Table 92. CP-8(2): Telecommunication Service

CP-8(2): Telecommunication Service		
Control		
The organization obtains alternate telecommunications services with consideration for reducing the likelihood of sharing a single point of failure with primary telecommunications services.		
Guidance		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.7	**Related Control Requirements:**
Assessment Procedure: CP-8(2).1		
Assessment Objective		
Determine if the organization obtains alternate telecommunications services with consideration for reducing the likelihood of sharing a single point of failure with primary telecommunications services.		
Assessment Methods and Objects		
Examine: Contingency planning policy; contingency plan; procedures addressing alternate telecommunications services; primary and alternate telecommunications service agreements; other relevant documents or records.		
Interview: Organizational personnel with contingency planning and plan implementation responsibilities; telecommunications service providers.		

Table 93. CP-9: Information System Backup

CP-9: Information System Backup
Control
The organization: a. Conducts backups of user-level information contained in the information system in accordance with the frequency specified in Implementation Standard 1; b. Conducts backups of system-level information contained in the information system in accordance with the frequency specified in Implementation Standard 1; c. Conducts backups of information system documentation including security-related documentation and other forms of data, including paper records; and d. Protects the confidentiality and integrity of Exchange backup information at the storage location.

CP-9: Information System Backup

Implementation Standards

1. Perform full backups weekly to separate media. Perform incremental or differential backups daily to separate media. Backups to include user-level and system-level information (including system state information). Three (3) generations of backups (full plus all related incremental or differential backups) are stored off-site. Off-site and on-site backups must be logged with name, date, time and action.
2. (For PII only) Ensure that a current, retrievable, copy of PII is available before movement of servers.

   For FTI: Back-up tapes must be labeled as containing FTI, must be logged, must be transported securely using two barriers and a transmittal, and must be inventoried on a semi-annual basis.

Guidance

System-level information includes, for example, system-state information, operating system and application software, and licenses. Digital signatures and cryptographic hashes are examples of mechanisms that can be employed by organizations to protect the integrity of information system backups. An organizational assessment of risk guides the use of encryption for protecting backup information. The protection of system backup information while in transit is beyond the scope of this control.

The transfer rate of backup information to an alternate storage site (if so designated) is guided by the Exchange recovery time objectives and recovery point objectives. Checkpoint capabilities are part of any backup operation that updates files and consumes large amounts of information system time.

Applicability: Exchanges	**Reference(s):** HIPAA: 164.308(a)(7)(ii)(A), 164.312(c)(1); IRS-1075: 3.0, 4.0, 9.7	**Related Control Requirements:** MP-4

Assessment Procedure: CP-9.1

Assessment Objective

Determine if:

(i) the organization backs up user-level information in accordance with the frequency specified in Implementation Standard 1;

(ii) the organization backs up system-level information in accordance with the frequency specified in Implementation Standard 1;

(iii) the organization backs up information system documentation (including security-related information and other forms of data).

(iv) the organization meets all the requirements specified in the applicable implementation standard(s).

Assessment Methods and Objects

Examine: Contingency planning policy; contingency plan; procedures addressing information system backup; security plan; backup storage location(s); information system backup logs or records; other relevant documents or records.

Interview: Organizational personnel with information system backup responsibilities.

Assessment Procedure: CP-9.2

Assessment Objective

Determine if the organization protects the confidentiality and integrity of backup information at the storage location.

Assessment Methods and Objects

Examine: Contingency planning policy; contingency plan; procedures addressing information system backup; information system design documentation; information system configuration settings and associated documentation; backup storage location(s); other relevant documents or records.

Interview: Organizational personnel with information system backup responsibilities.

Table 94. CP-9(1): Backup Testing

<table>
<tr><th colspan="3">CP-9(1): Backup Testing</th></tr>
<tr><td colspan="3"><b>Control</b></td></tr>
<tr><td colspan="3">The organization tests backup information following each backup to verify media reliability and information integrity.</td></tr>
<tr><td><b>Applicability:</b> Exchanges</td><td><b>Reference(s):</b> IRS-1075: 9.7</td><td><b>Related Control Requirements:</b></td></tr>
<tr><td colspan="3"><b>Assessment Procedure: CP-9(1).1</b></td></tr>
<tr><td colspan="3"><b>Assessment Objective</b></td></tr>
<tr><td colspan="3">Determine if:</td></tr>
<tr><td colspan="3">(i) the organization defines in the security plan, explicitly or by reference, the frequency of information system backup testing;
(ii) the organization conducts information system backup testing in accordance with organization-defined frequency to verify backup media reliability and information integrity.</td></tr>
<tr><td colspan="3"><b>Assessment Methods and Objects</b></td></tr>
<tr><td colspan="3"><b>Examine:</b> Contingency planning policy; contingency plan; procedures addressing information system backup; security plan; information system backup test results; backup storage location(s); other relevant documents or records.</td></tr>
</table>

Table 95. CP-10: Information System Recovery and Reconstitution

<table>
<tr><th colspan="3">CP-10: Information System Recovery and Reconstitution</th></tr>
<tr><td colspan="3"><b>Control</b></td></tr>
<tr><td colspan="3">The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure. Recovery of the information system after a failure or other contingency shall be done in a trusted, secure, and verifiable manner.</td></tr>
<tr><td colspan="3"><b>Implementation Standards</b></td></tr>
<tr><td colspan="3">1. Secure information system recovery and reconstitution includes, but not limited to:
a. Reset all system parameters (either default or organization-established),
b. Reinstall patches,
c. Reestablish configuration settings,
d. Reinstall application and system software, and
e. Fully test the system.</td></tr>
<tr><td colspan="3"><b>Guidance</b></td></tr>
<tr><td colspan="3">Recovery is executing information system contingency plan activities to restore essential missions and business functions. Reconstitution takes place following recovery and includes activities for returning the information system to its original functional state before contingency plan activation. Recovery and reconstitution procedures are based on priorities, established recovery point/time and reconstitution objectives, and appropriate metrics. Reconstitution includes the deactivation of any interim information system capability that may have been needed during recovery operations. Reconstitution also includes an assessment of the fully restored information system capability, a potential system reauthorization and the necessary activities to prepare the system against another disruption, compromise, or failure. Recovery and reconstitution capabilities employed by the organization can be a combination of automated mechanisms and manual procedures.</td></tr>
<tr><td><b>Applicability:</b> Exchanges</td><td><b>Reference(s):</b> HIPAA: 164.308(a)(7)(ii)(C); HSPD 7: G(22)(i)</td><td><b>Related Control Requirements:</b></td></tr>
<tr><td colspan="3"><b>Assessment Procedure: CP-10.1</b></td></tr>
<tr><td colspan="3"><b>Assessment Objective</b></td></tr>
<tr><td colspan="3">Determine if:</td></tr>
<tr><td colspan="3">(i) the organization provides automated mechanisms and/or manual procedures for the recovery and reconstitution of the information system to known state after a disruption, compromise, or failure;
(ii) the organization provides for the recovery of the information system after a failure or other contingency in a</td></tr>
</table>

CP-10: Information System Recovery and Reconstitution
trusted, secure, and verifiable manner. (iii) the organization meets all the requirements specified in the applicable implementation standard(s).
Assessment Methods and Objects
Examine: Contingency planning policy; contingency plan; procedures addressing information system recovery and reconstitution; information system configuration settings and associated documentation; information system design documentation; other relevant documents or records.

Table 96. CP-10(2): Information System Recovery and Reconstitution

CP-10(2): Information System Recovery and Reconstitution		
Control		
The information system implements transaction recovery for systems that are transaction-based. Enhancement Supplemental Guidance: Database management systems and transaction processing systems are examples of information systems that are transaction-based. Transaction rollback and transaction journaling are examples of mechanisms supporting transaction recovery.		
Applicability: Exchanges	**Reference(s):**	**Related Control Requirements:**
Assessment Procedure: CP-10(2).1		
Assessment Objective		
Determine if the information system implements transaction recovery for systems that are transaction-based.		
Assessment Methods and Objects		
Examine: Contingency planning policy; contingency plan; procedures addressing information system recovery and reconstitution; information system design documentation; information system configuration settings and associated documentation; contingency plan test results; other relevant documents or records.		

Table 97. CP-10(3): Information System Recovery and Reconstitution

CP-10(3): Information System Recovery and Reconstitution		
Control		
The organization provides compensating security controls for circumstances that inhibit recovery and reconstitution to a known state.		
Applicability: Exchanges	**Reference(s):**	**Related Control Requirements:**
Assessment Procedure: CP-10(3).1		
Assessment Objective		
Determine if:		
(i) the organization defines in the security plan, explicitly or by reference, the circumstances that can inhibit recovery and reconstitution of the information system to a known state; and (ii) the organization provides compensating security controls for organization-defined circumstances that can inhibit recovery and reconstitution of the information system to a known state.		
Assessment Methods and Objects		
Examine: Contingency planning policy; contingency plan; procedures addressing information system recovery and reconstitution; contingency plan test procedures; security plan; other relevant documents or records.		
Interview: Organizational personnel with information system recovery and reconstitution responsibilities.		

Identification and Authentication (IA) – Technical

Table 98. IA-1: Identification and Authentication Policy and Procedures

IA-1: Identification and Authentication Policy and Procedures		
Control		
The organization develops, disseminates, and reviews/updates within every three-hundred-sixty-five (365) days: a. A formal, documented identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.		
Guidance		
This control is intended to produce the policy and procedures that are required for the effective implementation of security controls and control enhancements in the identification and authentication family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The identification and authentication policy can be included as part of the general information security policy for the organization. Identification and authentication procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the identification and authentication policy.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.8	**Related Control Requirements:**
Assessment Procedure: IA-1.1		
Assessment Objective		
Determine if:		
(i) the organization develops and formally documents identification and authentication policy; (ii) the organization identification and authentication policy addresses: – scope; – roles and responsibilities; – management commitment; – coordination among organizational entities; – compliance; (iii) the organization disseminates formal documented identification and authentication policy to elements within the organization having associated identification and authentication roles and responsibilities; (iv) the organization develops and formally documents identification and authentication procedures; (v) the organization identification and authentication procedures facilitate implementation of the identification and authentication policy and associated identification and authentication controls; (vi) the organization disseminates formal documented identification and authentication procedures to elements within the organization having associated identification and authentication roles and responsibilities; (vii) the organization reviews/updates the identification and authentication policy and procedures within every three-hundred-sixty-five (365) days.		
Assessment Methods and Objects		
Examine: Identification and authentication policy and procedures; other relevant documents or records.		
Interview: Organizational personnel with identification and authentication responsibilities.		

Table 99. IA-2: Identification and Authentication (Organizational Users)

<table>
<tr><th colspan="3">IA-2: Identification and Authentication (Organizational Users)</th></tr>
<tr><td colspan="3"><b>Control</b></td></tr>
<tr><td colspan="3">The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).</td></tr>
<tr><td colspan="3"><b>Implementation Standards</b></td></tr>
<tr><td colspan="3">1. Require the use of system and/or network authenticators and unique user identifiers.
2. Help desk support requires user identification for any transaction that has information security implications.
For FTI: Complete section 2.10 (e-Authentication level) in the SSP Template.</td></tr>
<tr><td colspan="3"><b>Guidance</b></td></tr>
<tr><td colspan="3">Organizational users (i.e., information system users) include organizational employees or individuals the organization deems to have equivalent status of employees (e.g., contractors, guest researchers, individuals from allied nations). Users are uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization. Unique identification of individuals in group accounts (e.g., shared privilege accounts) may need to be considered for detailed accountability of activity. Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination thereof. Access to information systems is defined as either local or network.
Local access is any access to an information system by a user (or process acting on behalf of a user) where such access is obtained by direct connection without the use of a network. Network access is any access to an information system by a user (or process acting on behalf of a user) where such access is obtained through a network connection. Remote access is a type of network access which involves communication through an external network (e.g., the Internet). Internal networks include local area networks, wide area networks, and virtual private networks that are under the control of the organization. For a virtual private network (VPN), the VPN is considered an internal network if the organization establishes the VPN connection between organization-controlled endpoints in a manner that does not require the organization to depend on any external networks across which the VPN transits to protect the confidentiality and integrity of information transmitted. Identification and authentication requirements for information system access by other than organizational users are described in IA-8.
In addition to identifying and authenticating users at the information-system level (i.e., at logon), identification and authentication mechanisms are employed at the application level, when necessary, to provide increased information security for the organization.</td></tr>
<tr><td><b>Applicability:</b> Exchanges</td><td><b>Reference(s):</b> HIPAA: 164.312(a)(2)(i), 164.312(d); IRS-1075: 9.8</td><td><b>Related Control Requirements:</b> AC-17</td></tr>
<tr><td colspan="3"><b>Assessment Procedure: IA-2.1</b></td></tr>
<tr><td colspan="3"><b>Assessment Objective</b></td></tr>
<tr><td colspan="3">Determine if:</td></tr>
<tr><td colspan="3">(i) the information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).
(ii) the organization meets all the requirements specified in the applicable implementation standard(s).</td></tr>
<tr><td colspan="3"><b>Assessment Methods and Objects</b></td></tr>
<tr><td colspan="3"><b>Examine:</b> Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; information system audit records; list of information system accounts; other relevant documents or records.</td></tr>
</table>

Table 100. IA-2(1): Privileged Accounts Multifactor Authentication

IA-2(1): Privileged Accounts Multifactor Authentication		
Control		
The information system uses multifactor authentication for network access to privileged accounts. For FTI: Two-factor authentication is required whenever FTI is being accessed from an alternative work location or if accessing FTI via agency’s web portal by an employee or contractor.		
Applicability: Exchanges	**Reference(s):** HIPAA: 164.312(d); IRS-1075: 9.8	**Related Control Requirements:**
Assessment Procedure: IA-2(1).1		
Assessment Objective		
Determine if:		
(i) the information system uses multifactor authentication for network access to privileged accounts.		
Assessment Methods and Objects		
Examine: Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; list of privileged information system accounts; other relevant documents or records.		

Table 101. IA-2(2): Non-Privileged Accounts Multifactor Authentication

IA-2(2): Non-Privileged Accounts Multifactor Authentication		
Control		
The information system uses multifactor authentication for network access to non-privileged accounts.		
Applicability: Exchanges	**Reference(s):**	**Related Control Requirements:**
Assessment Procedure: IA-2(2).1		
Assessment Objective		
Determine if:		
(i) the information system uses multifactor authentication for network access to non-privileged accounts.		
Assessment Methods and Objects		
Examine: Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; list of non-privileged information system accounts; other relevant documents or records.		

Table 102. IA-2(3): Non-Privileged Accounts Multifactor Authentication

IA-2(3): Non-Privileged Accounts Multifactor Authentication		
Control		
The information system uses multifactor authentication for local access to privileged accounts.		
Applicability: Exchanges	**Reference(s):**	**Related Control Requirements:**
Assessment Procedure: IA-2(3).1		
Assessment Objective		
Determine if the information system uses multifactor authentication for local access to privileged accounts.		
Assessment Methods and Objects		
Examine: Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; list of privileged information system accounts; other relevant documents or records.		

Table 103. IA-2(8): Non-Privileged Accounts Multifactor Authentication

<table>
<tr><th colspan="3">IA-2(8): Non-Privileged Accounts Multifactor Authentication</th></tr>
<tr><td colspan="3"><b>Control</b></td></tr>
<tr><td colspan="3">The information system uses replay resistant authentication mechanisms for network access to privileged accounts.</td></tr>
<tr><td colspan="3"><b>Guidance</b></td></tr>
<tr><td colspan="3">An authentication process resists replay attacks if it is impractical to achieve a successful authentication by recording and replaying a previous authentication message. Techniques used to address this include protocols that use nonces or challenges (e.g., TLS), and time synchronous or challenge-response one-time authenticators.</td></tr>
<tr><td><b>Applicability:</b> Exchanges</td><td><b>Reference(s):</b></td><td><b>Related Control Requirements:</b></td></tr>
<tr><td colspan="3"><b>Assessment Procedure: IA-2(8).1</b></td></tr>
<tr><td colspan="3"><b>Assessment Objective</b></td></tr>
<tr><td colspan="3">Determine if:</td></tr>
<tr><td colspan="3">(i) the organization defines the replay-resistant authentication mechanisms to be used for network access to privileged accounts; and
(ii) the information system uses the organization-defined replay-resistant authentication mechanisms for network access to privileged accounts.</td></tr>
<tr><td colspan="3"><b>Assessment Methods and Objects</b></td></tr>
<tr><td colspan="3"><b>Examine:</b> Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; list of privileged information system accounts; other relevant documents or records.</td></tr>
</table>

Table 104. IA-3: Device Identification and Authentication

<table>
<tr><th colspan="3">IA-3: Device Identification and Authentication</th></tr>
<tr><td colspan="3"><b>Control</b></td></tr>
<tr><td colspan="3">The information system uniquely identifies and authenticates specific and/or types of devices before establishing a connection.</td></tr>
<tr><td colspan="3"><b>Guidance</b></td></tr>
<tr><td colspan="3">The devices requiring unique identification and authentication may be defined by type, by specific device, or by a combination of type and device as deemed appropriate by the organization. The information system typically uses either shared known information (e.g., Media Access Control [MAC] or Transmission Control Protocol/Internet Protocol [TCP/IP] addresses) for identification or an organizational authentication solution (e.g., IEEE 802.1x and Extensible Authentication Protocol [EAP], Radius server with EAP-Transport Layer Security [TLS] authentication, Kerberos) to identify and authenticate devices on local and/or wide area networks. The required strength of the device authentication mechanism is determined by the security categorization of the information system.</td></tr>
<tr><td><b>Applicability:</b> Exchanges</td><td><b>Reference(s):</b> IRS-1075: 9.8</td><td><b>Related Control Requirements:</b></td></tr>
<tr><td colspan="3"><b>Assessment Procedure: IA-3.1</b></td></tr>
<tr><td colspan="3"><b>Assessment Objective</b></td></tr>
<tr><td colspan="3">Determine if:</td></tr>
<tr><td colspan="3">(i) the organization defines the specific and/or types of devices for which identification and authentication is required before establishing a connection to the information system; and
(ii) the information system uniquely identifies and authenticates the organization-defined devices before establishing a connection to the information system.</td></tr>
<tr><td colspan="3"><b>Assessment Methods and Objects</b></td></tr>
<tr><td colspan="3"><b>Examine:</b> Identification and authentication policy; procedures addressing device identification and authentication; information system design documentation; list of devices requiring unique identification and authentication; device connection reports; information system configuration settings and associated documentation; other relevant documents or records.</td></tr>
</table>

Table 105. IA-4: Identifier Management

IA-4: Identifier Management

Control

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

a. Receiving authorization from a designated organizational official to assign a user or device identifier;

b. Selecting an identifier that uniquely identifies an individual or device;

c. Assigning the user identifier to the intended party or the device identifier to the intended device;

d. Preventing reuse of user or device identifiers until all previous access authorizations are removed from the system, including all file accesses for that identifier but not before a period of at least three hundred sixty-five (365) days has expired; and

e. Disabling the user identifier after the time period of inactivity specified in Implementation Standard 1 and deleting disabled accounts during the annual re-certification process.

Implementation Standard

1. Disable user identifiers after one hundred eighty (180) days of inactivity.

For FTI: Disable user identifier after ninety (90) days of inactivity.

Guidance

Common device identifiers include media access control (MAC) or Internet protocol (IP) addresses, or device-unique token identifiers. Management of user identifiers is not applicable to shared information system accounts (e.g., guest and anonymous accounts). It is commonly the case that a user identifier is the name of an information system account associated with an individual. In such instances, identifier management is largely addressed by the account management activities of AC-2. IA-4 also covers user identifiers not necessarily associated with an information system account (e.g., the identifier used in a physical security control database accessed by a badge reader system for access to the information system).

Applicability: Exchanges	**Reference(s):** IRS-1075: 9.8	**Related Control Requirements:** AC-2, IA-2

Assessment Procedure: IA-4.1

Assessment Objective

Determine if:

(i) the organization defines the time period for preventing reuse of user or device identifiers;

(ii) the organization defines the time period of inactivity after which a user identifier is to be disabled; and

(iii) the organization manages information system identifiers for users and devices by:

– receiving authorization from a designated organizational official to assign a user or device identifier;

– selecting an identifier that uniquely identifies an individual or device;

– assigning the user identifier to the intended party or the device identifier to the intended device;

– preventing reuse of user or device identifiers for the organization-defined time period; and

– disabling the user identifier after the organization-defined time period of inactivity.

Assessment Methods and Objects

Examine: Identification and authentication policy; procedures addressing identifier management; procedures addressing account management; security plan; information system design documentation; information system configuration settings and associated documentation; list of information system accounts; list of identifiers generated from physical access control devices; other relevant documents or records.

Table 106. IA-5: Authenticator Management

IA-5: Authenticator Management

Control

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

a. Verifying, as part of the initial authenticator distribution, the identity of the individual and/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;

IA-5: Authenticator Management

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 upon information system installation;

f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if appropriate);

g. Changing/refreshing password authenticators as defined organizational password policy

h. Protecting authenticator content from unauthorized disclosure and modification; and

i. Requiring users to take, and having devices implement, specific measures to safeguard authenticators.

Guidance

User 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). Many information system components are shipped with factory default authentication credentials to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, present a significant security risk, and therefore, are changed upon installation. The requirement to protect user authenticators may be implemented via policy or access agreements for authenticators in the possession of users and by controls AC-3, AC-6, and SC-28 for authenticators stored within the information system (e.g., passwords stored in a hashed or encrypted format, files containing encrypted or hashed passwords accessible only with super user privileges). The information system supports user authenticator management by security 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 verification stage of biometric authentication. Measures to safeguard user authenticators include, for example, maintaining possession of individual authenticators, not loaning or sharing authenticators with others, and reporting lost 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.

Applicability: Exchanges	**Reference(s):** IRS-1075: 9.8, Exhibit 8	**Related Control Requirements:**

Assessment Procedure: IA-5.1

Assessment Objective

Determine if:

(i) the organization defines the time period (by authenticator type) for changing/refreshing authenticators

(ii) the organization manages information system authenticators for users and devices by:

- verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator;
- establishing initial authenticator content for authenticators defined by the organization;
- ensuring that authenticators have sufficient strength of mechanism for their intended use;
- establishing and implementing administrative procedures for initial authenticator distribution;
- establishing and implementing administrative procedures for lost/compromised or damaged authenticators;
- establishing and implementing administrative procedures for revoking authenticators;
- changing default content of authenticators upon information system installation;
- establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if deemed to be appropriate by the organization);
- changing/refreshing authenticators in accordance with the organization-defined time period by authenticator type;
- protecting authenticator content from unauthorized disclosure and modification;
- requiring users to take, and having devices implement, specific measures to safeguard authenticators.

Assessment Methods and Objects

Examine: Identification and authentication policy; procedures addressing authenticator management; information system design documentation; information system configuration settings and associated documentation; list of information system accounts; other relevant documents or records.

Interview: Organizational personnel with responsibilities for determining initial authenticator content.

Table 107. IA-5(1): Authenticator Management

IA-5(1): Authenticator Management		
Control		
The information system, for password-based authentication: a. Automatically forces users (including administrators) to change user account passwords every sixty (60) days and system account passwords every one hundred eighty (180) days; b. Prohibits the use of dictionary names or words; c. Enforces minimum password complexity consisting of at least eight (8) alphanumeric (i.e., upper- and lower-case letters, and numbers) and/or special characters; d. Enforces at least a minimum of four (4) changed characters when new passwords are created; e. Encrypts passwords in storage and in transmission; f. Enforces password minimum and maximum lifetime restrictions of one (1) day for the minimum, and sixty (60) days for a user account and one hundred eighty (180) days for a system account maximum; and g. Prohibits password reuse for six (6) generations prior to reuse. For FTI: Change/refresh authenticators every 90 days, at a minimum, for a standard user account, every 60 days, at a minimum, for privileged users.		
Guidance		
This control enhancement is intended primarily for environments where passwords are used as a single factor to authenticate users, or in a similar manner along with one or more additional authenticators. The enhancement generally does *not* apply to situations where passwords are used to unlock hardware authenticators. The implementation of such password mechanisms may not meet all of the requirements in the enhancement.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.8	**Related Control Requirements:**
Assessment Procedure: IA-5(1).1		
Assessment Objective		
Determine if:		
(i) the organization defines the minimum password complexity requirements to be enforced for case sensitivity, the number of characters, and the mix of upper-case letters, lower-case letters, numbers, and special characters including minimum requirements for each type; (ii) the organization defines the minimum number of characters that must be changed when new passwords are created;		
(iii) the organization defines the restrictions to be enforced for password minimum lifetime and password maximum lifetime parameters; (iv) the organization defines the number of generations for which password reuse is prohibited; and (v) the information system, for password-based authentication: – enforces the minimum password complexity standards that meet the organization-defined requirements; – enforces the organization-defined minimum number of characters that must be changed when new passwords are created; – encrypts passwords in storage and in transmission; – enforces the organization-defined restrictions for password minimum lifetime and password maximum lifetime parameters; and – prohibits password reuse for the organization-defined number of generations.		
Assessment Methods and Objects		
Examine: Identification and authentication policy; password policy; procedures addressing authenticator management; security plan; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.		

Table 108. IA-5(2): Authenticator Management

IA-5(2): Authenticator Management		
Control		
The information system, for PKI-based authentication: a. Validates certificates by constructing a certification path with status information to an accepted trust anchor; b. Enforces authorized access to the corresponding private key; and c. Maps the authenticated identity to the user account.		
Guidance		
Status information for certification paths includes, for example, certificate revocation lists or online certificate status protocol responses.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.8	**Related Control Requirements:**
Assessment Procedure: IA-5(2).1		
Assessment Objective		
Determine if the information system, for PKI-based authentication: (i) validates certificates by constructing a certification path with status information to an accepted trust anchor; (ii) enforces authorized access to the corresponding private key; and (iii) maps the authenticated identity to the user account.		
Assessment Methods and Objects		
Examine: Identification and authentication policy; procedures addressing authenticator management; security plan; information system design documentation; information system configuration settings and associated documentation; PKI certification revocation lists; other relevant documents or records.		
Interview: Organizational personnel with responsibilities for PKI-based authentication management.		

Table 109. IA-5(3): Authenticator Management

IA-5(3): Authenticator Management		
Control		
The organization requires that the registration process to receive hardware tokens be verified in person before a designated registration authority with authorization by a designated organizational official (e.g., a supervisor).		
Guidance		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.8	**Related Control Requirements:**
Assessment Procedure: IA-5(3).1		
Assessment Objective		
Determine if:		
(i) the organization defines the types of and/or specific authenticators for which the registration process must be carried out in person before a designated registration authority with authorization by a designated organizational official; and (ii) the organization requires that the registration process to receive organizationdefined types of and/or specific authenticators be carried out in person before a designated registration authority with authorization by a designated organizational official (e.g., a supervisor).		
Assessment Methods and Objects		
Examine: Identification and authentication policy; procedures addressing authenticator management; list of authenticators that require in-person registration; authenticator registration documentation; other relevant documents or records.		
Interview: Organizational personnel with authenticator management responsibilities.		

Table 110. IA-6: Authenticator Feedback

IA-6: Authenticator Feedback		
Control		
The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.		
Guidance		
The feedback from the information system does not provide information that would allow an unauthorized user to compromise the authentication mechanism. Displaying asterisks when a user types in a password, is an example of obscuring feedback of authentication information.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.8	**Related Control Requirements:**
Assessment Procedure: IA-6.1		
Assessment Objective		
Determine if the information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.		
Assessment Methods and Objects		
Examine: Identification and authentication policy; procedures addressing authenticator feedback; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.		

Table 111. IA-7: Cryptographic Module Authentication

IA-7: Cryptographic Module Authentication		
Control		
The information system uses 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.		
Guidance		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.8	**Related Control Requirements:**
Assessment Procedure: IA-5.1		
Assessment Objective		
Determine if the information system uses 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.		
Assessment Methods and Objects		
Examine: Identification and authentication policy; procedures addressing cryptographic module authentication; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.		

Table 112. IA-8: Identification and Authentication (Non-Organizational Users)

IA-8: Identification and Authentication (Non-Organizational Users)
Control
The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).

IA-8: Identification and Authentication (Non-Organizational Users)		
Guidance		
Non-organizational users include all Exchange information system users other than organizational users explicitly covered by IA-2. Users are uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization. Accordingly, a risk assessment is used in determining the authentication needs of the organization. Scalability, practicality, and security are simultaneously considered in balancing the need to ensure ease of use for access to information and information systems with the need to protect and adequately mitigate risk to the organization's operations, assets, individuals, and other organizations. Identification and authentication requirements for information system access by organizational users are described in IA-2. If E-Authentication is used, refer to NIST SP 800-63 Electronic Authentication Guideline.		
Applicability: Exchanges	**Reference(s):**	**Related Control Requirements:**
Assessment Procedure: IA-8.1		
Assessment Objective		
Determine if the information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).		
Assessment Methods and Objects		
Examine: Determine if the information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).		
Interview: Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; information system audit records; list of information system accounts; other relevant documents or records.		

Incident Response (IR) – Operational

Table 113. IR-1: Incident Response Policy and Procedures

IR-1: Incident Response Policy and Procedures		
Control		
The organization develops, disseminates, and reviews/updates within every three-hundred-sixty-five (365) days: a. A formal, documented incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls. For FTI: Policies and procedures must cover both physical and information security relative to the protection of FTI.		
Guidance		
This control is intended to produce the policy and procedures that are required for the effective implementation of security controls and control enhancements in the incident response family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The incident response policy can be included as part of the general information security policy for the organization. Incident response procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the incident response policy.		
Applicability: Exchanges	**Reference(s):** HIPAA: 164.308(a)(6)(i); IRS-1075: 9.9	**Related Control Requirements:**
Assessment Procedure: IR-1.1		
Assessment Objective		
Determine if:		
(i) the organization develops and formally documents incident response policy; (ii) the organization incident response policy addresses: – purpose; – scope; – roles and responsibilities; – management commitment; – coordination among organizational entities; – compliance; (iii) the organization disseminates formal documented incident response policy to elements within the organization having associated incident response roles and responsibilities; (iv) the organization develops and formally documents incident response procedures; (v) the organization incident response procedures facilitate implementation of the incident response policy and associated incident response controls; (vi) the organization disseminates formal documented incident response procedures to elements within the organization having associated incident response roles and responsibilities; (vii) the organization reviews/updates the incident response policy and procedures within every three-hundred-sixty-five (365) days.		
Assessment Methods and Objects		
Examine: Incident response policy and procedures; other relevant documents or records.		
Interview: Organizational personnel with incident response responsibilities.		

Table 114. IR-2: Incident Response Training

IR-2: Incident Response Training

Control

The organization:

a. Trains personnel in their incident response roles and responsibilities with respect to the information system; and
b. Provides refresher training within every three-hundred-sixty-five (365) days.

For FTI: Provides refresher training prior to access of FTI and annually thereafter on incident response policy and procedure regarding FTI.

Supplemental Guidance:

Incident response training includes user training in the identification and reporting of suspicious activities, both from external and internal sources.

Guidance

Incident response training includes user training in the identification and reporting of suspicious activities, both from external and internal sources. Incident response training implementation should:

a. Identify employees with significant information security responsibilities and provide role-specific training in accordance with National Institute of Standards and Technology (NIST) standards and guidance:
   1. All users of information systems must be exposed to security awareness materials at least annually. Users of information systems include employees, contractors, students, guest researchers, visitors, and others who may need access to information systems and applications.
   2. Executives must receive training in information security basics and policy level training in security planning and management.
   3. Program and functional managers must receive training in information security basics; management and implementation level training in security planning and system/application security management; and management and implementation level training in system/application life cycle management, risk management, and contingency planning.
   4. CIOs, IT security program managers, auditors, and other security-oriented personnel (e.g., system and network administrators, and system/application security officers) must receive training in information security basics and broad training in security planning, system and application security management, system/application life cycle management, risk management, and contingency planning.
   5. IT function management and operations personnel must receive training in information security basics; management and implementation level training in security planning and system/application security management; and management and implementation level training in system/ application life cycle management, risk management, and contingency planning.
b. Provide the information systems security awareness material/exposure outlined in NIST guidance on IT security awareness and training to all new employees before allowing them access to the systems.
c. Provide information systems security refresher training for employees as frequently as determined necessary, based on the sensitivity of the information that the employees use or process.
d. Provide training whenever there is a significant change in the information system environment or procedures or when an employee enters a new position that requires additional role-specific training.

Applicability: Exchanges	**Reference(s):** IRS-1075: 6.2, 9.9	**Related Control Requirements:**

Assessment Procedure: IR-2.1

Assessment Objective

Determine if:

(i) the organization identifies personnel with incident response roles and responsibilities with respect to the information system;
(ii) the organization provides incident response training to personnel with incident response roles and responsibilities with respect to the information system;
(iii) incident response training material addresses the procedures and activities necessary to fulfill identified organizational incident response roles and responsibilities;
(iv) the organization defines in the security plan, explicitly or by reference, the frequency of refresher incident response training and the frequency is at least annually;
(v) the organization provides refresher incident response training in accordance with organization-defined

IR-2: Incident Response Training
frequency.
Assessment Methods and Objects
Examine: Incident response policy; procedures addressing incident response training; incident response training material; security plan; incident response plan; incident response training records; other relevant documents or records.
Interview: Organizational personnel with incident response training and operational responsibilities.

Table 115. IR-3: Incident Response Testing and Exercises

<table>
<tr><th colspan="3">IR-3: Incident Response Testing and Exercises</th></tr>
<tr><td colspan="3"><b>Control</b></td></tr>
<tr><td colspan="3">The organization tests and/or exercises the incident response capability for the information system annually using reviews, analyses, and simulations to determine the incident response effectiveness and documents the results.
For FTI: Include procedures to exercise responding to unauthorized FTI access and reporting unauthorized FTI access to IRS and TIGTA.</td></tr>
<tr><td colspan="3"><b>Guidance</b></td></tr>
<tr><td colspan="3"></td></tr>
<tr><td><b>Applicability:</b> Exchanges</td><td><b>Reference(s):</b> IRS-1075: 9.9</td><td><b>Related Control Requirements:</b></td></tr>
<tr><td colspan="3"><b>Assessment Procedure: IR-3.1</b></td></tr>
<tr><td colspan="3"><b>Assessment Objective</b></td></tr>
<tr><td colspan="3">Determine if:</td></tr>
<tr><td colspan="3">(i) the organization defines incident response tests/exercises;
(ii) the organization defines the frequency of incident response tests/exercises;
(iii) the organization tests/exercises the incident response capability for the information system using organization-defined tests/exercises in accordance with organization-defined frequency;
(iv) the organization documents the results of incident response tests/exercises; and
(v) the organization determines the effectiveness of the incident response capability.</td></tr>
<tr><td colspan="3"><b>Assessment Methods and Objects</b></td></tr>
<tr><td colspan="3"><b>Examine:</b> Incident response policy; procedures addressing incident response testing and exercises; security plan; incident response testing material; incident response test results; incident response plan; other relevant documents or records.</td></tr>
<tr><td colspan="3"><b>Interview:</b> Organizational personnel with incident response testing responsibilities.</td></tr>
</table>

Table 116. IR-4: Incident Handling

IR-4: Incident Handling
Control
The organization: a. Implements an incident handling capability using Information Security Incident Handling and Breach Notification Procedures; 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/exercises, and implements the resulting changes accordingly. For FTI: The agency's incident response policy and procedures must include specific guidance relative to a data incidents involving FTI.
Implementation Standard(s)
1. Document relevant information related to a security incident according to Information Security Incident

<table>
<tr><th colspan="3">IR-4: Incident Handling</th></tr>
<tr><td colspan="3">Handling and Breach Notification Procedures.
2. Preserve evidence through technical means, including secured storage of evidence media and "write" protection of evidence media. Use sound forensics processes and utilities that support legal requirements. Determine and follow chain of custody for forensic evidence.
3. Identify vulnerability exploited during a security incident. Implement security safeguards to reduce risk and vulnerability exploit exposure.</td></tr>
<tr><td colspan="3"><b>Guidance</b></td></tr>
<tr><td colspan="3">Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.</td></tr>
<tr><td><b>Applicability:</b> Exchanges</td><td><b>Reference(s):</b> HIPAA: 164.308(a)(6)(ii); IRS-1075: 9.9</td><td><b>Related Control Requirements:</b> AU-6</td></tr>
<tr><td colspan="3"><b>Assessment Procedure: IR-4.1</b></td></tr>
<tr><td colspan="3"><b>Assessment Objective</b></td></tr>
<tr><td colspan="3">Determine if:</td></tr>
<tr><td colspan="3">(i) the organization implements an incident handling capability for security incidents that includes:
– preparation;
– detection and analysis;
– containment;
– eradication;
– recovery;
(ii) the organization coordinates incident handling activities with contingency planning activities;
(iii) the organization incorporates lessons learned from ongoing incident handling activities into:
– incident response procedures;
– training;
– testing/exercises;
(iv) the organization implements the resulting changes to incident response procedures, training and testing/exercise accordingly.
(v) the organization meets all the requirements specified in the applicable implementation standard(s).</td></tr>
<tr><td colspan="3"><b>Assessment Methods and Objects</b></td></tr>
<tr><td colspan="3"><b>Examine:</b> Incident response policy; procedures addressing incident handling; incident response plan; other relevant documents or records.</td></tr>
<tr><td colspan="3"><b>Interview:</b> Organizational personnel with incident handling responsibilities; organizational personnel with contingency planning responsibilities.</td></tr>
</table>

Table 117. IR-4(1): Incident Handling

<table>
<tr><th colspan="3">IR-4(1): Incident Handling</th></tr>
<tr><td colspan="3"><b>Control</b></td></tr>
<tr><td colspan="3">The organization employs automated mechanisms to support the incident handling process.</td></tr>
<tr><td colspan="3"><b>Guidance</b></td></tr>
<tr><td colspan="3">An online incident management system is an example of an automated mechanism.</td></tr>
<tr><td><b>Applicability:</b> Exchanges</td><td><b>Reference(s):</b> IRS-1075: 9.9</td><td><b>Related Control Requirements:</b></td></tr>
<tr><td colspan="3"><b>Assessment Procedure: IR-4(1).1</b></td></tr>
<tr><td colspan="3"><b>Assessment Objective</b></td></tr>
<tr><td colspan="3">Determine if the organization employs automated mechanisms to support the incident handling process.</td></tr>
<tr><td colspan="3"><b>Assessment Methods and Objects</b></td></tr>
<tr><td colspan="3"><b>Examine:</b> Incident response policy; procedures addressing incident handling; automated mechanisms supporting incident handling; other relevant documents or records.</td></tr>
</table>

IR-4(1): Incident Handling
Interview: Organizational personnel with incident handling responsibilities.

Table 118. IR-5: Incident Monitoring

IR-5: Incident Monitoring		
Control		
The organization tracks and documents information system security incidents.		
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. For FTI: Once the incident has been addressed, the agency will conduct a post-incident review to ensure the incident response policies and procedures provide adequate guidance. (Pub 1075 section 10.3) For FTI: Complete SPR section 9.11.5		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.9, 10.4	**Related Control Requirements:**
Assessment Procedure: IR-5.1: Incident Monitoring		
Assessment Objective		
Determine if the organization tracks and documents information system security incidents.		
Assessment Methods and Objects		
Examine: Incident response policy; procedures addressing incident reporting; incident reporting records and documentation; incident response plan; other relevant documents or records.		
Interview: Organizational personnel with incident monitoring responsibilities.		

Table 119. IR-6: Incident Reporting

IR-6: Incident Reporting		
Control		
The organization: a. Requires personnel to report suspected security incidents to the organizational incident response capability within timeframe established in the current Information Security Incident Handling and Breach Analysis/Notification Procedure; and b. Reports security incident information to designated authorities. For FTI: Any data incident potentially involving FTI must immediately be reported to the Treasury Inspector General for Tax Administration (TIGTA) and the IRS Office of Safeguards immediately, but no later than 24-hours after identification of a possible issue involving FTI.		
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. The types of security incidents reported, the content and timeliness of the reports, and the list of designated reporting authorities are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, 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.		
Applicability:	**Reference(s):** IRS-1075: 9.9, 10.4	**Related Control Requirements:** IR-4,

IR-6: Incident Reporting		
Exchanges		IR-5
Assessment Procedure: IR-6.1		
Assessment Objective		
Determine if:		
(i) the organization requires personnel to report suspected security incidents to the organizational incident response capability within the timeframe established in the current Information Security Incident Handling and Breach Analysis/Notification Procedure; (ii) the organization reports security incident information to designated authorities.		
Assessment Methods and Objects		
Examine: Incident response policy; procedures addressing incident reporting; incident reporting records and documentation; security plan; incident response plan; other relevant documents or records.		
Interview: Organizational personnel with incident reporting responsibilities.		

Table 120. IR-6(1): Incident Reporting

IR-6(1): Incident Reporting		
Control		
The organization employs automated mechanisms to assist in the reporting of security incidents.		
Guidance		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.9	**Related Control Requirements:**
Assessment Procedure: IR-6(1).1		
Assessment Objective		
Determine if the organization employs automated mechanisms to assist in the reporting of security incidents.		
Assessment Methods and Objects		
Examine: Incident response policy; procedures addressing incident reporting; automated mechanisms supporting incident reporting; incident response plan; other relevant documents or records.		
Interview: Organizational personnel with incident reporting responsibilities.		

Table 121. IR-7: Incident Response Assistance

IR-7: Incident Response Assistance		
Control		
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. For FTI: The agency shall provide an incident response support resource that offers advice and assistance to users of the federal tax information and any information system containing federal tax information for the handling and reporting of security incidents. The support resource is an integral part of the agency's incident response capability.		
Guidance		
Possible implementations of incident response support resources in an organization include a help desk or an assistance group and access to forensics services, when required.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.9	**Related Control Requirements:**

IR-7: Incident Response Assistance
Assessment Procedure: IR-7.1
Assessment Objective
Determine if:
(i) the organization provides an incident response support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents; and (ii) the incident response support resource is an integral part of the organization's incident response capability.
Assessment Methods and Objects
Examine: Incident response policy; procedures addressing incident response assistance; incident response plan; other relevant documents or records.
Interview: Organizational personnel with incident response assistance and support responsibilities.

Table 122. IR-7(1): Incident Response Assistance

IR-7(1): Incident Response Assistance		
Control		
The organization employs automated mechanisms to increase the availability of incident response-related information and support.		
Guidance		
Automated mechanisms can provide a push and/or pull capability for users to obtain incident response assistance. For example, individuals might have access to a website to query the assistance capability, or conversely, the assistance capability may have the ability to proactively send information to users (general distribution or targeted) as part of increasing understanding of current response capabilities and support.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.9	**Related Control Requirements:**
Assessment Procedure: IR-7(1).1		
Assessment Objective		
Determine if the organization employs automated mechanisms to increase the availability of incident response-related information and support.		
Assessment Methods and Objects		
Examine: Incident response policy; procedures addressing incident response assistance; automated mechanisms supporting incident response support and assistance; incident response plan; other relevant documents or records.		
Interview: Organizational personnel with incident response support and assistance responsibilities; organizational personnel that require incident response support and assistance.		

Table 123. IR-8: Incident Response Plan

IR-8: Incident Response Plan
Control
The organization: a. Develops an incident response plan that: – Provides the organization with a roadmap for implementing its incident response capability; – Describes the structure and organization of the incident response capability; – Provides a high-level approach for how the incident response capability fits into the overall organization; – Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; – Defines reportable incidents; – Provides metrics for measuring the incident response capability within the organization. – Defines the resources and management support needed to effectively maintain and mature an incident response capability; and

IR-8: Incident Response Plan

   – Is reviewed and approved by designated officials within the organization;

b. Distributes copies of the incident response plan to incident response personnel and organizational elements;

c Reviews the incident response plan within every three-hundred-sixty-five (365) days;

d Revises the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; and

e. Communicates incident response plan changes to incident response personnel and organizational elements.

For FTI: The agency shall agency develop, document, and maintain a current incident response plan that describes the structure and organization of the incident response capability and includes incident response procedures specific to FTI.

Guidance

It is important that organizations have a formal, focused, and coordinated approach to responding to incidents. The organization's mission, strategies, and goals for incident response help determine the structure of its incident response capability.

Applicability: Exchanges	**Reference(s):** IRS-1075: 9.9	**Related Control Requirements:**

Assessment Procedure: IR-8.1

Assessment Objective

Determine if the organization develops an incident response plan that:

(i) provides the organization with a roadmap for implementing its incident response capability;
(ii) describes the structure and organization of the incident response capability;
(iii) provides a high-level approach for how the incident response capability fits into the overall organization;
(iv) meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
(v) defines reportable incidents;
(vi) provides metrics for measuring the incident response capability within the organization;
(vii) defines the resources and management support needed to effectively maintain and mature an incident response capability;
(viii) is reviewed and approved by designated officials within the organization.

Assessment Methods and Objects

Examine: Incident response policy; procedures addressing incident response assistance; incident response plan; other relevant documents or records.

Interview: Organizational personnel with incident response planning responsibilities.

Assessment Procedure: IR-8.2

Assessment Objective

Determine if:

(i) the organization defines, in the incident response plan, incident response personnel (identified by name and/or role) and organizational elements;
(ii) the organization distributes copies of the incident response plan to incident response personnel and organizational elements identified in the plan;
(iii) the organization reviews the incident response plan in accordance with the organization-defined frequency;
(iv) the organization revises the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing;
(v) the organization communicates incident response plan changes to incident response personnel and organizational elements identified in the plan.

Assessment Methods and Objects

Examine: Incident response policy; procedures addressing incident response assistance; incident response plan; other relevant documents or records.

Interview: Organizational personnel with incident response planning responsibilities.

Maintenance (MA) – Operational

Table 124. MA-1: System Maintenance Policy and Procedures

<table>
<tr><th colspan="3">MA-1: System Maintenance Policy and Procedures</th></tr>
<tr><td colspan="3"><b>Control</b></td></tr>
<tr><td colspan="3">The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:
a. A formal, documented information system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
b. Formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.</td></tr>
<tr><td colspan="3"><b>Guidance</b></td></tr>
<tr><td colspan="3">This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the system maintenance family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The information system maintenance policy can be included as part of the general information security policy for the organization. System maintenance procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the system maintenance policy.</td></tr>
<tr><td><b>Applicability:</b> Exchanges</td><td><b>Reference(s):</b> IRS-1075: 9.10</td><td><b>Related Control Requirements:</b> PM-9</td></tr>
<tr><td colspan="3"><b>Assessment Procedure: MA-1.1</b></td></tr>
<tr><td colspan="3"><b>Assessment Objective</b></td></tr>
<tr><td colspan="3">Determine if:</td></tr>
<tr><td colspan="3">(i) the organization develops and formally documents system maintenance policy;
(ii) the organization system maintenance policy addresses:
– purpose;
– scope;
– roles and responsibilities;
– management commitment;
– coordination among organizational entities; and
– compliance;
(iii) the organization disseminates formal documented system maintenance policy to elements within the organization having associated system maintenance roles and responsibilities;
(iv) the organization develops and formally documents system maintenance procedures;
(v) the organization system maintenance procedures facilitate implementation of the system maintenance policy and associated system maintenance controls; and
(vi) the organization disseminates formal documented system maintenance procedures to elements within the organization having associated system maintenance roles and responsibilities.</td></tr>
<tr><td colspan="3"><b>Assessment Methods and Objects</b></td></tr>
<tr><td colspan="3"><b>Examine:</b> Information system maintenance policy and procedures; other relevant documents or records.</td></tr>
<tr><td colspan="3"><b>Interview:</b> Organizational personnel with information system maintenance responsibilities.</td></tr>
</table>

Table 125. MA-2: Controlled Maintenance

MA-2: Controlled Maintenance		
Control		
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. Controls 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 a designated official 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; and e. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.		
Implementation Standard		
1. (For PII only) In facilities where PII is stored or accessed, document repairs and modifications to the physical components of a facility that are related to security (for example, hardware, walls, doors, and locks).		
Guidance		
The control is intended to address the information security aspects of the organization's information system maintenance program.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.10	**Related Control Requirements:** MP-6, SI-2
Assessment Procedure: MA-2.1		
Assessment Objective		
Determine if:		
(i) the organization 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; (ii) the organization controls all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location; (iii) the organization requires that a designated official explicitly approve the removal of the information system or system components from organizational facilities for offsite maintenance or repairs; (iv) the organization sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs; and (v) the organization checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.		
Assessment Methods and Objects		
Examine: Information system maintenance policy; procedures addressing controlled maintenance for the information system; maintenance records; manufacturer/vendor maintenance specifications; equipment sanitization records; media sanitization records; other relevant documents or records.		
Interview: Organizational personnel with information system maintenance responsibilities.		

Table 126. MA-2(1): Controlled Maintenance

MA-2(1): Controlled Maintenance		
Control		
The organization maintains maintenance records for the information system that include: a. date and time of maintenance; b. name of the individual performing the maintenance; c. name of escort, if necessary; d. a description of the maintenance performed; e. a list of equipment removed or replaced (including identification numbers, if applicable).		
Guidance		
Applicability: Exchanges	**Reference(s): I**RS-1075: 9.10	**Related Control Requirements:**
Assessment Procedure: MA-2(1).1		
Assessment Objective		
Determine if the organization maintains maintenance records for the information system that include: (i) date and time of maintenance; (ii) name of the individual performing the maintenance; (iii) name of escort, if necessary; (iv) a description of the maintenance performed; and (v) a list of equipment removed or replaced (including identification numbers, if applicable).		
Assessment Methods and Objects		
Examine: Information system maintenance policy; procedures addressing controlled maintenance for the information system; maintenance records; other relevant documents or records.		

Table 127. MA-3: Maintenance Tools

MA-3: Maintenance Tools		
Control		
The organization approves, controls, monitors the use of, and maintains on an ongoing basis, information system maintenance tools.		
Guidance		
The intent of this control is to address the security-related issues arising from the hardware and software brought into the information system specifically for diagnostic and repair actions (e.g., a hardware or software packet sniffer that is introduced for the purpose of a particular maintenance activity). Hardware and/or software components that may support information system maintenance, yet are a part of the system (e.g., the software implementing “ping,” “ls,” “ipconfig,” or the hardware and software implementing the monitoring port of an Ethernet switch) are not covered by this control.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.10	**Related Control Requirements:** MP-6
Assessment Procedure: MA-3.1		
Assessment Objective		
Determine if:		
(i) the organization approves, controls, and monitors the use of information system maintenance tools; and (ii) the organization maintains information system maintenance tools on an ongoing basis.		
Assessment Methods and Objects		
Examine: Information system maintenance policy; information system maintenance tools and associated documentation; procedures addressing information system maintenance tools; maintenance records; other relevant documents or records.		

Table 128. MA-3(1): Maintenance Tools

MA-3(1): Maintenance Tools		
Control		
The organization inspects all maintenance tools carried into a facility by maintenance personnel for obvious improper modifications**.**		
Guidance		
Maintenance tools include, for example, diagnostic and test equipment used to conduct maintenance on the information system.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.10	**Related Control Requirements:**
Assessment Procedure: MA-3(1).1		
Assessment Objective		
Determine if the organization inspects all maintenance tools carried into a facility by maintenance personnel for obvious improper modifications.		
Assessment Methods and Objects		
Examine: Information system maintenance policy; information system maintenance tools and associated documentation; procedures addressing information system maintenance tools; maintenance records; other relevant documents or records.		
Interview: Organizational personnel with information system maintenance responsibilities.		

Table 129. MA-3(2): Maintenance Tools

MA-3(2): Maintenance Tools		
Control		
The organization checks all media containing diagnostic and test programs for malicious code before the media are used in the information system.		
Guidance		
Applicability: Exchanges	**Reference(s): I**RS-1075: 9.10	**Related Control Requirements:**
Assessment Procedure: MA-3(2).1		
Assessment Objective		
Determine if the organization checks all media containing diagnostic and test programs (e.g., software or firmware used for information system maintenance or diagnostics) for malicious code before the media are used in the information system.		
Assessment Methods and Objects		
Examine: Information system maintenance policy; information system maintenance tools and associated documentation; procedures addressing information system maintenance tools; information system media containing maintenance programs (including diagnostic and test programs); maintenance records; other relevant documents or records.		
Interview: Organizational personnel with information system maintenance responsibilities.		

Table 130. MA-4: Non-Local Maintenance

<table>
<tr><th colspan="3">MA-4: Non-Local Maintenance</th></tr>
<tr><td colspan="3"><b>Control</b></td></tr>
<tr><td colspan="3">The organization prohibits non-local system maintenance unless explicitly authorized, in writing, by the CIO or his/her designated representative. If authorized, the organization:
a. Monitors and controls non-local maintenance and diagnostic activities;
b. Allows the use of non-local maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system;
c. Employs strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions;
d. Maintains records for non-local maintenance and diagnostic activities; and
e. Terminates all sessions and network connections when non-local maintenance is completed.</td></tr>
<tr><td colspan="3"><b>Implementation Standard</b></td></tr>
<tr><td colspan="3">If password-based authentication is used during remote maintenance, change the passwords following each remote maintenance service.</td></tr>
<tr><td colspan="3"><b>Guidance</b></td></tr>
<tr><td colspan="3">Non-local 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. Identification and authentication techniques used in the establishment of non-local maintenance and diagnostic sessions are consistent with the network access requirements in IA-2. 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.</td></tr>
<tr><td><b>Applicability:</b> Exchanges</td><td><b>Reference(s):</b> IRS-1075: 9.10</td><td><b>Related Control Requirements:</b> AC-2, AC-3, AC-6, AC-17, AU-2, AU-3, IA-2, IA-8, MA-5, MP-6, SC-7.</td></tr>
<tr><td colspan="3"><b>Assessment Procedure: MA-4.1</b></td></tr>
<tr><td colspan="3"><b>Assessment Objective</b></td></tr>
<tr><td colspan="3">Determine if:</td></tr>
<tr><td colspan="3">(i) the organization authorizes, monitors, and controls non-local maintenance and diagnostic activities;
(ii) the organization documents, in the organizational policy and security plan for the information system, the acceptable conditions for allowing the use of non-local maintenance and diagnostic tools;
(iii) the organization allows the use of non-local maintenance and diagnostic tools only as consistent with organizational policy and as documented in the security plan;
(iv) the organization employs strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions;
(v) the organization maintains records for non-local maintenance and diagnostic activities; and
(vi) the organization (or information system in certain cases) terminates all sessions and network connections when non-local maintenance or diagnostics is completed.</td></tr>
<tr><td colspan="3"><b>Assessment Methods and Objects</b></td></tr>
<tr><td colspan="3"><b>Examine:</b> Information system maintenance policy; procedures addressing non-local maintenance for the information system; security plan; information system design documentation; information system configuration settings and associated documentation; maintenance records; other relevant documents or records.</td></tr>
<tr><td colspan="3"><b>Interview:</b> Organizational personnel with information system maintenance responsibilities.</td></tr>
</table>

Table 131. MA-4(1): Non-Local Maintenance

<table>
<tr><th colspan="3">MA-4(1): Non-Local Maintenance</th></tr>
<tr><td colspan="3"><b>Control</b></td></tr>
<tr><td colspan="3">The organization audits non-local maintenance and diagnostic sessions and designated organizational personnel review the maintenance records of the sessions.</td></tr>
<tr><td colspan="3"><b>Guidance</b></td></tr>
<tr><td colspan="3"></td></tr>
<tr><td><b>Applicability:</b> Exchanges</td><td><b>Reference(s):</b> IRS-1075: 9.10</td><td><b>Related Control Requirements:</b></td></tr>
<tr><td colspan="3"><b>Assessment Procedure: MA-4(1).1</b></td></tr>
<tr><td colspan="3"><b>Assessment Objective</b></td></tr>
<tr><td colspan="3">Determine if:</td></tr>
<tr><td colspan="3">(i) the organization audits non-local maintenance and diagnostic sessions; and
(ii) designated organizational personnel review the maintenance records of the sessions.</td></tr>
<tr><td colspan="3"><b>Assessment Methods and Objects</b></td></tr>
<tr><td colspan="3"><b>Examine:</b> Information system maintenance policy; procedures addressing non-local maintenance for the information system; maintenance records; audit records; other relevant documents or records.</td></tr>
<tr><td colspan="3"><b>Interview:</b> Organizational personnel with information system maintenance responsibilities.</td></tr>
</table>

Table 132. MA-4(2): Non-Local Maintenance

<table>
<tr><th colspan="3">MA-4(2): Non-Local Maintenance</th></tr>
<tr><td colspan="3"><b>Control</b></td></tr>
<tr><td colspan="3">The organization documents, in the security plan for the information system, the installation and use of non-local maintenance and diagnostic connections.</td></tr>
<tr><td colspan="3"><b>Guidance</b></td></tr>
<tr><td colspan="3"></td></tr>
<tr><td><b>Applicability:</b> Exchanges</td><td><b>Reference(s):</b> IRS-1075: 9.10</td><td><b>Related Control Requirements:</b></td></tr>
<tr><td colspan="3"><b>Assessment Procedure: MA-4(2).1</b></td></tr>
<tr><td colspan="3"><b>Assessment Objective</b></td></tr>
<tr><td colspan="3">Determine if the organization documents the installation and use of non-local maintenance and diagnostic connections in the security plan for the information system.</td></tr>
<tr><td colspan="3"><b>Assessment Methods and Objects</b></td></tr>
<tr><td colspan="3"><b>Examine:</b> Information system maintenance policy; procedures addressing non-local maintenance for the information system; security plan; maintenance records; audit records; other relevant documents or records.</td></tr>
</table>

Table 133. MA-4(3): Non-Local Maintenance

MA-4(3): Non-Local Maintenance		
Control		
The organization: a. Requires that non-local maintenance and diagnostic services be performed from an information system that implements a level of security at least as high as that implemented on the system being serviced; or b. Removes the component to be serviced from the information system and prior to non-local maintenance or diagnostic services, sanitizes the component (with regard to sensitive information such as FTI or Privacy Act protected information) before removal from organizational facilities, and after the service is performed, inspects and sanitizes the component (with regard to potentially malicious software and surreptitious implants) before reconnecting the component to the information system.		
Guidance		
Applicability: Exchanges	**Reference(s): I**RS-1075: 9.10	**Related Control Requirements:**
Assessment Procedure: MA-4(3).1		
Assessment Objective		
Determine if:		
(i) the organization requires and ensures non-local maintenance and diagnostic services are performed from an information system that implements a level of security at least as high as the level of security implemented on the information system being serviced; or (ii) the organization removes the component to be serviced from the information system and prior to non-local maintenance or diagnostic services, sanitizes the component (with regard to organizational information) before removal from organizational facilities; and (iii) the organization after the removed component service is performed, inspects and sanitizes the component (with regard to potentially malicious software and surreptitious implants) before reconnecting to the information system.		
Assessment Methods and Objects		
Examine: Information system maintenance policy; procedures addressing non-local maintenance for the information system; service provider contracts and/or service level agreements; maintenance records; audit records; other relevant documents or records.		
Interview: Organizational personnel with information system maintenance responsibilities; information system maintenance provider.		

Table 134. MA-5: Maintenance Personnel

MA-5: Maintenance Personnel
Control
The organization: a. Establishes a process for maintenance personnel authorization and maintains a current list of authorized maintenance organizations or personnel; and b. Ensures that personnel performing maintenance on the information system have required access authorizations or designates organizational personnel with required access authorizations and technical competence deemed necessary to supervise information system maintenance when maintenance personnel do not possess the required access authorizations.
Guidance
Individuals not previously identified in the information system, such as vendor personnel and consultants, may legitimately require privileged access to the system, for example, when required to conduct maintenance or diagnostic activities with little or no notice. Based on a prior assessment of risk, the organization may issue temporary credentials to these individuals. Temporary credentials may be for one-time use or for a very limited time period.

MA-5: Maintenance Personnel		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.10	**Related Control Requirements:** IA-8, MA-5
Assessment Procedure: MA-5.1		
Assessment Objective		
Determine if:		
(i) the organization establishes a process for maintenance personnel authorization; (ii) the organization maintains a current list of authorized maintenance organizations or personnel; and (iii) personnel performing maintenance on the information system either have the required access authorizations or are supervised by designated organizational personnel with the required access authorizations and technical competence deemed necessary to supervise information system maintenance.		
Assessment Methods and Objects		
Examine: Information system maintenance policy; procedures addressing maintenance personnel; service provider contracts and/or service level agreements; list of authorized personnel; maintenance records; access control records; other relevant documents or records.		
Interview: Organizational personnel with information system maintenance responsibilities.		

Table 135. MA-6: Timely Maintenance

MA-6: Timely Maintenance		
Control		
The organization obtains maintenance support and/or spare parts for critical systems and applications (including Major Applications [MA] and General Support Systems [GSS] and their components) within twenty-four (24) hours of failure.		
Guidance		
The organization specifies those information system components that, when not operational, result in increased risk to organizations, individuals, or the Nation because the security functionality intended by that component is not being provided. Security-critical components include, for example, firewalls, guards, gateways, intrusion detection systems, audit repositories, authentication servers, and intrusion prevention systems.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.10	**Related Control Requirements:** CP-2
Assessment Procedure: MA-6.1		
Assessment Objective		
Determine if:		
(i) the organization defines security-critical information system components and/or key information technology components for which it will obtain maintenance support and/or spare parts; (ii) the organization defines the time period within which support and/or spare parts must be obtained after a failure; and (iii) the organization obtains maintenance support and/or spare parts for the organization-defined list of security-critical information system components and/or key information technology components within the organization-defined time period of failure.		
Assessment Methods and Objects		
Examine: Information system maintenance policy; procedures addressing timely maintenance for the information system; service provider contracts and/or service level agreements; inventory and availability of spare parts; security plan; other relevant documents or records.		
Interview: Organizational personnel with information system maintenance responsibilities.		

Media Protection (MP) – Operational

Table 136. MP-1: Media Protection Policy and Procedures

<table>
<tr><th colspan="3">MP-1: Media Protection Policy and Procedures</th></tr>
<tr><td colspan="3"><b>Control</b></td></tr>
<tr><td colspan="3">The organization develops, disseminates, and reviews/updates within every three-hundred-sixty-five (365) days:
a. A formal, documented media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
b. Formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.</td></tr>
<tr><td colspan="3"><b>Implementation Standards</b></td></tr>
<tr><td colspan="3">1. (For PII only) Semi-annual inventories of magnetic tapes containing PII are conducted. The organization accounts for any missing tape containing PII by documenting the search efforts and notifying the tape initiator of the loss.</td></tr>
<tr><td colspan="3"><b>Guidance</b></td></tr>
<tr><td colspan="3">This control is intended to produce the policy and procedures that are required for the effective implementation of Exchange security controls and control enhancements in the media protection family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The media protection policy can be included as part of the general information security policy for the organization. Media protection procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the media protection policy.</td></tr>
<tr><td><b>Applicability:</b> Exchanges</td><td><b>Reference(s):</b> HIPAA: 164.310(d)(1); IRS-1075: 9.11</td><td><b>Related Control Requirements:</b></td></tr>
<tr><td colspan="3"><b>Assessment Procedure: MP-1.1</b></td></tr>
<tr><td colspan="3"><b>Assessment Objective</b></td></tr>
<tr><td colspan="3">Determine if:</td></tr>
<tr><td colspan="3">(i) the organization develops and formally documents media protection policy;
(ii) the organization media protection policy addresses:
– purpose;
– scope;
– roles and responsibilities;
– management commitment;
– coordination among organizational entities;
– compliance
(iii) the organization disseminates formal documented media protection policy to elements within the organization having associated media protection roles and responsibilities;
(iv) the organization develops and formally documents media protection procedures;
(v) the organization media protection procedures facilitate implementation of the media protection policy and associated media protection controls
(vi) the organization disseminates formal documented media protection procedures to elements within the organization having associated media protection roles and responsibilities.
(vii) the organization reviews/updates the media protection policy and procedures within every three-hundred-sixty-five (365) days.
(viii) the organization meets all the requirements specified in the applicable implementation standard(s).</td></tr>
<tr><td colspan="3"><b>Assessment Methods and Objects</b></td></tr>
<tr><td colspan="3"><b>Examine:</b> Media protection policy and procedures; other relevant documents or records.</td></tr>
<tr><td colspan="3"><b>Examine:</b> PII semiannual inventory reports; other relevant documents or records.</td></tr>
<tr><td colspan="3"><b>Interview:</b> Organizational personnel with information system media protection responsibilities.</td></tr>
</table>

Table 137. MP-2: Media Access

<table>
<tr><th colspan="3">MP-2: Media Access</th></tr>
<tr><td colspan="3"><b>Control</b></td></tr>
<tr><td colspan="3">The organization restricts access to sensitive (such as FTI or Private Act protected information) residing on digital and non-digital media to authorized individuals using automated mechanisms to control access to media storage areas.</td></tr>
<tr><td colspan="3"><b>Guidance</b></td></tr>
<tr><td colspan="3">Information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). This control also applies to mobile computing and communications devices with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices). An organizational assessment of risk guides the selection of media and associated information contained on that media requiring restricted access. Organizations document in policy and procedures, the media requiring restricted access, individuals authorized to access the media, and the specific measures taken to restrict access. Fewer protection measures are needed for media containing information determined by the organization to be in the public domain, to be publicly releasable, or to have limited or no adverse impact if accessed by other than authorized personnel. In these situations, it is assumed that the physical access controls where the media resides provide adequate protection.</td></tr>
<tr><td><b>Applicability:</b> Exchanges</td><td><b>Reference(s):</b> HIPAA: 164.308(a)(3)(ii)(A), 164.312(c)(1); IRS-1075: 4.6#1, 6.3.3#1</td><td><b>Related Control Requirements:</b></td></tr>
<tr><td colspan="3"><b>Assessment Procedure: MP-2.1</b></td></tr>
<tr><td colspan="3"><b>Assessment Objective</b></td></tr>
<tr><td colspan="3">Determine if:</td></tr>
<tr><td colspan="3">(i) the organization defines:
– digital and non-digital media requiring restricted access;
– individuals authorized to access the media;
– security measures taken to restrict access;
(ii) the organization restricts access to organization-defined information system media to organization-defined authorized individuals using organization-defined security measures.</td></tr>
<tr><td colspan="3"><b>Assessment Methods and Objects</b></td></tr>
<tr><td colspan="3"><b>Examine:</b> Information system media protection policy; procedures addressing media access; access control policy and procedures; physical and environmental protection policy and procedures; media storage facilities; access control records; other relevant documents or records.</td></tr>
<tr><td colspan="3"><b>Interview:</b> Organizational personnel with information system media protection responsibilities.</td></tr>
</table>

Table 138. MP-2(1): Media Access

<table>
<tr><th colspan="3">MP-2(1): Media Access</th></tr>
<tr><td colspan="3"><b>Control</b></td></tr>
<tr><td colspan="3">The organization employs automated mechanisms to restrict access to media storage areas and to audit access attempts and access granted.</td></tr>
<tr><td colspan="3"><b>Guidance</b></td></tr>
<tr><td colspan="3">This control enhancement is primarily applicable to media storage areas within an organization where a significant volume of media is stored and is not applicable to every location where some media is stored (e.g., in individual offices).</td></tr>
<tr><td><b>Applicability:</b> Exchanges</td><td><b>Reference(s): I</b>RS-1075: 9.11</td><td><b>Related Control Requirements:</b></td></tr>
<tr><td colspan="3"><b>Assessment Procedure: MP-2(1).1</b></td></tr>
<tr><td colspan="3"><b>Assessment Objective</b></td></tr>
<tr><td colspan="3">Determine if:</td></tr>
</table>

<table>
<tr><th>MP-2(1): Media Access</th></tr>
<tr><td>(i) the organization employs automated mechanisms to restrict access to media storage areas; and
(ii) the organization employs automated mechanisms to audit access attempts and access granted to media storage areas.</td></tr>
<tr><td><b>Assessment Methods and Objects</b></td></tr>
<tr><td><b>Examine:</b> Information system media protection policy; procedures addressing media access; access control policy and procedures; physical and environmental protection policy and procedures; media storage facilities; access control devices; access control records; audit records; other relevant documents or records.</td></tr>
</table>

Table 139. MP-3: Media Marking

<table>
<tr><th colspan="3">MP-3: Media Marking</th></tr>
<tr><td colspan="3"><b>Control</b></td></tr>
<tr><td colspan="3">The organization:
a. Marks, in accordance with organizational policies and procedures, removable information system media and information system output indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and
b. Exempts specific types of media or hardware components, as specified, in writing, by the CIO or his/her designated representative, from marking as long as the exempted items remain within a secure environment.
For FTI: The agency must label removable media and information system output containing FTI. IRS Notice 129-A or Notice 129-B are available for this purpose.</td></tr>
<tr><td colspan="3"><b>Guidance</b></td></tr>
<tr><td colspan="3">The term marking is used when referring to the application or use of human-readable security attributes. The term labeling is used when referring to the application or use of security attributes with regard to internal data structures within the information system. Removable information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). An organizational assessment of risk guides the selection of media requiring marking. Marking is generally not required for media containing information determined by the organization to be in the public domain or to be publicly releasable. Organizations may extend the scope of this control to include information system output devices containing sensitive information (such as FTI or Privacy Act information), including, for example, monitors and printers.</td></tr>
<tr><td><b>Applicability:</b> Exchanges</td><td><b>Reference(s):</b> IRS-1075: 9.11</td><td><b>Related Control Requirements:</b></td></tr>
<tr><td colspan="3"><b>Assessment Procedure: MP-3.1</b></td></tr>
<tr><td colspan="3"><b>Assessment Objective</b></td></tr>
<tr><td colspan="3">Determine if:</td></tr>
<tr><td colspan="3">(i) the organization defines removable media types and information system output that require marking;
(ii) the organization marks removable media and information system output in accordance with organizational policies and procedures, indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information;
(iii) the organization defines:
– removable media types and information system output exempt from marking;
– controlled areas designated for retaining removable media and information output exempt from marking;
(iv) removable media and information system output exempt from marking remain within designated controlled areas.</td></tr>
<tr><td colspan="3"><b>Assessment Methods and Objects</b></td></tr>
<tr><td colspan="3"><b>Examine:</b> Information system media protection policy; procedures addressing media labeling; physical and environmental protection policy and procedures; security plan; removable storage media and information system output; other relevant documents or records.</td></tr>
<tr><td colspan="3"><b>Interview:</b> Organizational personnel with information system media protection and marking responsibilities.</td></tr>
</table>

Table 140. MP-4: Media Storage

MP-4: Media Storage

Control

The organization:

a. Physically controls and securely stores digital and non-digital media within controlled areas using safeguards prescribed for the highest system security level of the information ever recorded on it;

b. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

Implementation Standards

1. (For PII only) Evaluate employing an approved method of cryptography (see SC-13) to protect PII at rest, consistent with NIST SP 800-66 guidance.
2. (For PII only) If PII is recorded on magnetic media with other data, it should be protected as if it were entirely personally identifiable information.

Guidance

Information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). This control also applies to mobile computing and communications devices with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices). A controlled area is any area or space for which the organization has confidence that the physical and procedural protections are sufficient to meet the requirements established for protecting information and/or information system.

An organizational assessment of risk guides the selection of media and associated information contained on that media requiring physical protection. Fewer protection measures are needed for media containing information determined by the organization to be in the public domain, to be publicly releasable, or to have limited or no adverse impact on the organization or individuals if accessed by other than authorized personnel. In these situations, it is assumed that the physical access controls to the facility where the media resides provide adequate protection.

As part of a defense-in-depth strategy, the organization considers routinely encrypting sensitive information at rest on selected secondary storage devices. The selection of the cryptographic mechanisms used is based upon maintaining the confidentiality and integrity of the information. The strength of mechanisms is commensurate with the classification and sensitivity of the information.

Applicability: Exchanges	**Reference(s):** IRS-1075: 9.11	**Related Control Requirements:**

Assessment Procedure: MP-4.1

Assessment Objective

Determine if:

(i) the organization defines:
- types of digital and non-digital media physically controlled and securely stored within designated controlled areas;
- controlled areas designated to physically control and securely store the media;
- security measures to physically control and securely store the media within designated controlled areas;

(ii) the organization physically controls and securely stores information system media within organization-defined controlled areas using organization-defined security measures;

(iii) the organization protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

(iv) the organization meets all the requirements specified in the applicable implementation standard(s).

Assessment Methods and Objects

MP-4: Media Storage
Examine: Information system media protection policy; procedures addressing media storage; physical and environmental protection policy and procedures; access control policy and procedures; security plan; information system media; other relevant documents or records.
Examine: Cryptographic software licenses used to protect PII at rest.
Examine: PII magnetic media storage procedures.
Interview: Organizational personnel with PII protection responsibilities.
Interview: Organizational personnel with information system media protection and storage responsibilities.

Table 141. MP-5: Media Transport

<table>
<tr><th colspan="3">MP-5: Media Transport</th></tr>
<tr><td colspan="3"><b>Control</b></td></tr>
<tr><td colspan="3">The organization:
a. Protects and controls digital and non-digital media containing sensitive information (such as FTI or Privacy Act information) during transport outside of controlled areas using cryptography and tamper evident packaging and (i) if hand carried, using securable container (e.g., locked briefcase) via authorized personnel, or (ii) if shipped, trackable with receipt by commercial carrier;
b. Maintains accountability for information system media during transport outside of controlled areas; and
c. Restricts the activities associated with transport of such media to authorized personnel.
For FTI: All FTI transported through the mail or courier/messenger service must be double sealed; that is one envelope within another envelope. The inner envelope should be marked confidential with some indication that only the designated official or delegate is authorized to open it. Using sealed boxes serves the same purpose as double sealing and prevents anyone from viewing the contents thereof.</td></tr>
<tr><td colspan="3"><b>Guidance</b></td></tr>
<tr><td colspan="3">Information system media includes both digital media (e.g., diskettes, magnetic tapes, removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). This control also applies to mobile computing and communications devices with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices) that are transported outside of controlled areas. Telephone systems are also considered information systems and may have the capability to store information on internal media (e.g., on voicemail systems). Since telephone systems do not have, in most cases, the identification, authentication, and access control mechanisms typically employed in other information systems, organizational personnel use caution in the types of information stored on telephone voicemail systems that are transported outside of controlled areas. A controlled area is any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information system.
Physical and technical security measures for the protection of digital and non-digital media are commensurate with the classification or sensitivity of the information residing on the media, and consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Locked containers and cryptography are examples of security measures available to protect digital and non-digital media during transport. Cryptographic mechanisms can provide confidentiality and/or integrity protections depending upon the mechanisms used. An organizational assessment of risk guides: (i) the selection of media and associated information contained on that media requiring protection during transport; and (ii) the selection and use of storage containers for transporting non-digital media. 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).</td></tr>
<tr><td><b>Applicability:</b> Exchanges</td><td><b>Reference(s):</b> HIPAA: 164.308(a)(3)(ii)(A), 164.312(c)(1); IRS-1075: 9.11</td><td><b>Related Control Requirements:</b> AC-19, CP-9</td></tr>
<tr><td colspan="3"><b>Assessment Procedure: MP-5.1</b></td></tr>
</table>

MP-5: Media Transport
Assessment Objective
Determine if:
(i) the organization defines: – types of digital and non-digital media protected and controlled during transport outside of controlled areas; – security measures (e.g., locked container, encryption) for such media transported outside of controlled areas; (ii) the organization protects and controls organization-defined information system media during transport outside of controlled areas using organization-defined security measures; (iii) the organization maintains accountability for information system media during transport outside of controlled areas; (iv) the organization identifies personnel authorized to transport information system media outside of controlled areas; and (v) the organization restricts the activities associated with transport of information system media to authorized personnel.
Assessment Methods and Objects
Examine: Information system media protection policy; procedures addressing media transport; physical and environmental protection policy and procedures; access control policy and procedures; security plan; list of organization-defined personnel authorized to transport information system media outside of controlled areas; information system media; information system media transport records; information system audit records; other relevant documents or records.
Interview: Organizational personnel with information system media transport responsibilities.

Table 142. MP-5(2): Media Transport

MP-5(2): Media Transport		
Control		
The organization documents activities associated with the transport of information system media. For FTI: All shipments of FTI (including electronic media and microfilm) must be documented on a transmittal form and monitored to ensure that each shipment is properly and timely received and acknowledged.		
Implementation Standard		
For FTI: Describe the permanent record(s) (logs) used to document requests for, receipt of, distribution of (if applicable), and disposition (return to IRS or destruction) of the FTI (including tapes, cartridges or other removable media) (e.g. FTI receipt logs, transmission logs, or destruction logs in electronic or paper format) (Please include a sample of the agency logs as an attachment).		
Guidance		
Organizations establish documentation requirements for activities associated with the transport of information system media in accordance with the organizational assessment of risk to include the flexibility to define different record-keeping methods for different types of media transport as part of an overall system of transport-related records.		
Applicability: Exchanges	**Reference(s): I**RS-1075: 9.11	**Related Control Requirements:**
Assessment Procedure: MP-5(2).1		
Assessment Objective		
Determine if the organization documents activities associated with the transport of information system media.		
Assessment Methods and Objects		
Examine: Information system media protection policy; procedures addressing media transport; physical and environmental protection policy and procedures; access control policy and procedures; security plan; information system media transport records; audit records; other relevant documents or records.		

Table 143. MP-5(4): Media Transport

MP-5(4): Media Transport		
Control		
The organization employs cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.		
Guidance		
This control enhancement also applies to mobile devices. Mobile devices include portable storage media (e.g., USB memory sticks, external hard disk drives) and portable computing and communications devices with storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones).		
Applicability: Exchanges	**Reference(s): I**RS-1075: 9.11	**Related Control Requirements:**
Assessment Procedure: MP-5(4).1		
Assessment Objective		
Determine if the organization employs cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.		
Assessment Methods and Objects		
Examine: Information system media protection policy; procedures addressing media transport; information system media transport records; audit records; other relevant documents or records.		

Table 144. MP-6: Media Sanitization

MP-6: Media Sanitization
Control
The organization: a. Sanitizes information system media, both digital and non-digital, prior to disposal, release out of organizational control, or release for reuse; and b. Employs sanitization mechanisms with strength and integrity commensurate with the classification or sensitivity of the information. For FTI: 1. FTI furnished to the user and any paper material generated therefrom, such as extra copies, photo impressions, computer printouts, carbon paper, notes, stenographic notes, and work papers must be destroyed by burning, mulching, pulping, shredding, or disintegrating. 2. FTI must never be disclosed to an agency's agents or contractors during disposal unless authorized by the Internal Revenue Code. Generally, destruction should be witnessed by an agency employee.
Implementation Standard(s)
1. Finely shred, using a minimum of cross-cut shredding, hard-copy documents, using approved equipment, techniques, and procedures. 2. (For PII only) Authorized employees of the receiving entity must be responsible for securing magnetic tapes/cartridges before, during, and after processing, and they must ensure that the proper acknowledgment form is signed and returned. Inventory records must be maintained for purposes of control and accountability. Tapes containing PII, any hard-copy printout of a tape, or any file resulting from the processing of such a tape will be recorded in a log that identifies: – date received – reel/cartridge control number contents – number of records, if available – movement, and – if disposed of, the date and method of disposition. For FTI: The agency shall sanitize information system media prior to disposal or release for reuse.

MP-6: Media Sanitization		
Guidance		
This control applies to all media subject to disposal or reuse, whether or not considered removable. Sanitization is the process used to remove information from information system media such that there is reasonable assurance that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, and destroying media information, prevent the disclosure of organizational information to unauthorized individuals when such media is reused or released for disposal. The organization employs sanitization mechanisms with strength and integrity commensurate with the classification or sensitivity of the information. The organization uses its discretion on the employment of 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 the organization or individuals if released for reuse or disposal.		
Applicability: Exchanges	**Reference(s):** HIPAA: 164.308(a)(3)(ii)(A), 164.312(c)(1); IRS-1075: 8.3, 9.11	**Related Control Requirements:**
Assessment Procedure: MP-6.1		
Assessment Objective		
Determine if:		
(i) the organization sanitizes information system media both digital and non-digital prior to: – disposal; – release out of organizational control; or – release for reuse; and (ii) the organization employs sanitization mechanisms with strength and integrity commensurate with the classification or sensitivity of the information.		
Assessment Methods and Objects		
Examine: Information system media protection policy; procedures addressing media sanitization and disposal; media sanitization records; audit records; other relevant documents or records.		
Interview: Organizational personnel with information system media sanitization responsibilities.		

Table 145. MP-6(1): Media Sanitization

MP-6(1): Media Sanitization		
Control		
The organization tracks, documents, and verifies media sanitization and disposal actions.		
Guidance		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.11	**Related Control Requirements:**
Assessment Procedure: MP-6(1).1		
Assessment Objective		
Determine if the organization tracks, documents, and verifies media sanitization and disposal actions.		
Assessment Methods and Objects		
Examine: Information system media protection policy and procedures; media sanitization records; audit records; other relevant documents or records.		
Interview: Organizational personnel with information system media sanitization responsibilities.		

Table 146. MP-6(2): Media Sanitization

<table>
<tr><th colspan="3">MP-6(2): Media Sanitization</th></tr>
<tr><td colspan="3"><b>Control</b></td></tr>
<tr><td colspan="3">The organization tests sanitization equipment and procedures to verify correct performance periodically.</td></tr>
<tr><td colspan="3"><b>Guidance</b></td></tr>
<tr><td colspan="3"></td></tr>
<tr><td><b>Applicability:</b> Exchanges</td><td><b>Reference(s):</b> IRS-1075: 9.11</td><td><b>Related Control Requirements:</b></td></tr>
<tr><td colspan="3"><b>Assessment Procedure: MP-6(2).1</b></td></tr>
<tr><td colspan="3"><b>Assessment Objective</b></td></tr>
<tr><td colspan="3">Determine if:</td></tr>
<tr><td colspan="3">(i) the organization defines the frequency for testing sanitization equipment and procedures to verify correct performance; and
(ii) the organization tests sanitization equipment and procedures to verify correct performance in accordance with organization-defined frequency.</td></tr>
<tr><td colspan="3"><b>Assessment Methods and Objects</b></td></tr>
<tr><td colspan="3"><b>Examine:</b> Information system media protection policy; procedures addressing media sanitization and disposal; media sanitization equipment test records; information system audit records; other relevant documents or records.</td></tr>
<tr><td colspan="3"><b>Interview:</b> Organizational personnel with information system media sanitization responsibilities.</td></tr>
</table>

Table 147. MP-6(5): Media Sanitization

<table>
<tr><th colspan="3">MP-6(5): Media Sanitization</th></tr>
<tr><td colspan="3"><b>Control</b></td></tr>
<tr><td colspan="3">The organization sanitizes information system media containing sensitive information (such as FTI or Privacy Act protected information) using National Security Agency (NSA) guidance (www.nsa.gov/ia/government/mdg.cfm) and NIST SP 800-88, <i>Guidelines for Media Sanitization</i>.
For FTI: Electronic media containing FTI must not be made available for reuse by other offices or released for destruction without first being subject to electromagnetic erasing. If reuse is not intended, the electronic media should be destroyed. Whenever physical media leaves the physical or systemic control of the agency for maintenance, exchange or other servicing, any FTI on it must be cleared completely by overwriting all data tracks a minimum of three times.</td></tr>
<tr><td colspan="3"><b>Guidance</b></td></tr>
<tr><td colspan="3"></td></tr>
<tr><td><b>Applicability:</b> Exchanges</td><td><b>Reference(s):</b> IRS-1075: 8.3, 9.11</td><td><b>Related Control Requirements:</b></td></tr>
<tr><td colspan="3"><b>Assessment Procedure: MP-6(5).1</b></td></tr>
<tr><td colspan="3"><b>Assessment Objective</b></td></tr>
<tr><td colspan="3">Determine if the organization sanitizes information system media containing classified information in accordance with NSA standards and policies.</td></tr>
<tr><td colspan="3"><b>Assessment Methods and Objects</b></td></tr>
<tr><td colspan="3"><b>Examine:</b> Information system media protection policy and procedures; media sanitization records; audit records; other relevant documents or records.</td></tr>
<tr><td colspan="3"><b>Interview:</b> Organizational personnel with information system media sanitization responsibilities.</td></tr>
</table>

Table 148. MP-6(6): Media Sanitization

MP-6(6): Media Sanitization		
Control		
The organization destroys media containing sensitive information (such as FTI or Privacy Act protected information) that cannot be sanitized. For FTI: Paper FTI may be burned, cross-cut shredded to 5/16” wide or small strips or pulped.		
Guidance		
Applicability: Exchanges	**Reference(s): I**RS-1075: 8.3, 9.11	**Related Control Requirements:**
Assessment Procedure: MP-6(6).1		
Assessment Objective		
Determine if the organization implements the media destruction process for information system media that cannot be sanitized.		
Assessment Methods and Objects		
Examine: Information system media protection policy; procedures addressing media sanitization and disposal; media sanitization equipment test records; information system audit records; other relevant documents or records.		
Interview: Organizational personnel with information system media sanitization responsibilities.		

Table 149. MP-CMS-1: Media Related Records

MP-CMS-1: Media Related Records		
Control		
Inventory and disposition records for information system media shall be maintained to ensure control and accountability of CMS information. The media related records shall contain sufficient information to reconstruct the data in the event of a breach.		
Implementation Standard(s)		
1. The media records must, at a minimum, contain: a. The name of media recipient; b. Signature of media recipient; c. Date/time media received; d. Media control number and contents; e. Movement or routing information; and f. If disposed of, the date, time, and method of destruction.		
Guidance		
Applicability: Exchanges	**Reference(s):**	**Related Control Requirements:**
Assessment Procedure: MP-CMS-1		
Assessment Objective		
Determine if inventory and disposition records for information system media contain sufficient information to reconstruct the data in the event of a breach.		
Assessment Methods and Objects		
Examine: Inventory and disposition records for information system media		
Interview: Organizational personnel with information system media sanitization responsibilities.		

Physical and Environmental Protection (PE) – Operational

Table 150. PE-1: Physical and Environmental Protection Policy and Procedures

<table>
<tr><th colspan="3">PE-1: Physical and Environmental Protection Policy and Procedures</th></tr>
<tr><td colspan="3"><b>Control</b></td></tr>
<tr><td colspan="3">The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:
a. A formal, documented physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
b. Formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.</td></tr>
<tr><td colspan="3"><b>Guidance</b></td></tr>
<tr><td colspan="3">This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the physical and environmental protection family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The physical and environmental protection policy can be included as part of the general information security policy for the organization. Physical and environmental protection procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the physical and environmental protection policy.</td></tr>
<tr><td><b>Applicability:</b> Exchanges</td><td><b>Reference(s):</b> IRS-1075: 4.2</td><td><b>Related Control Requirements:</b> PM-9</td></tr>
<tr><td colspan="3"><b>Assessment Procedure: PE-1.1</b></td></tr>
<tr><td colspan="3"><b>Assessment Objective</b></td></tr>
<tr><td colspan="3">Determine if:</td></tr>
<tr><td colspan="3">(i) the organization develops and formally documents physical and environmental protection policy;
(ii) the organization physical and environmental protection policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities; and
- compliance;
(iii) the organization disseminates formal documented physical and environmental protection policy to elements within the organization having associated physical and environmental protection roles and responsibilities;
(iv) the organization develops and formally documents physical and environmental protection procedures;
(v) the organization physical and environmental protection procedures facilitate implementation of the physical and environmental protection policy and associated physical and environmental protection controls; and
(vi) the organization disseminates formal documented physical and environmental protection procedures to elements within the organization having associated physical and environmental protection roles and responsibilities.</td></tr>
<tr><td colspan="3"><b>Assessment Methods and Objects</b></td></tr>
<tr><td colspan="3"><b>Examine:</b> Physical and environmental protection policy and procedures; other relevant documents or records.</td></tr>
<tr><td colspan="3"><b>Interview:</b> Organizational personnel with physical and environmental protection responsibilities.</td></tr>
</table>

Table 151. PE-2: Physical Access Authorizations

<table>
<tr><th colspan="3">PE-2: Physical Access Authorizations</th></tr>
<tr><td colspan="3"><b>Control</b></td></tr>
<tr><td colspan="3">The organization:
a. Develops and keeps current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible);
b. Issues authorization credentials;
c. Reviews and approves the access list and authorization credentials in accordance with the frequency specified in Implementation Standard 1, removing from the access list personnel no longer requiring access.
For FTI: A visitor access log containing specific data elements will be used to authenticate and authorize visitor’s access to any facility where FTI resides, either electronically or in paper, at the location where the outside (2nd) barrier is breached.</td></tr>
<tr><td colspan="3"><b>Implementation Standards</b></td></tr>
<tr><td colspan="3">1. Review and approve lists of personnel with authorized access to facilities containing information systems at least once every one hundred eighty (180) days.
2. (For PII only) Create a restricted area, security room, or locked room to control access to areas containing PII. These areas will be controlled accordingly.</td></tr>
<tr><td colspan="3"><b>Guidance</b></td></tr>
<tr><td colspan="3">Authorization credentials include, for example, badges, identification cards, and smart cards.</td></tr>
<tr><td><b>Applicability:</b> Exchanges</td><td><b>Reference(s):</b> IRS-1075: 4.3.2</td><td><b>Related Control Requirements:</b> PE-3, PE-4</td></tr>
<tr><td colspan="3"><b>Assessment Procedure: PE-2.1</b></td></tr>
<tr><td colspan="3"><b>Assessment Objective</b></td></tr>
<tr><td colspan="3">Determine if:</td></tr>
<tr><td colspan="3">(i) the organization identifies areas within the facility that are publicly accessible;
(ii) the organization develops and keeps current lists of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible); and
(iii) the organization issues authorization credentials (e.g., badges, identification cards, smart cards).</td></tr>
<tr><td colspan="3"><b>Assessment Methods and Objects</b></td></tr>
<tr><td colspan="3"><b>Examine:</b> Physical and environmental protection policy; procedures addressing physical access authorizations; authorized personnel access list; authorization credentials; list of areas that are publicly accessible; other relevant documents or records.</td></tr>
<tr><td colspan="3"><b>Assessment Procedure: PE-2.2</b></td></tr>
<tr><td colspan="3"><b>Assessment Objective</b></td></tr>
<tr><td colspan="3">Determine if:</td></tr>
<tr><td colspan="3">(i) the organization defines the frequency for review and approval of the physical access list and authorization credentials for the facility;
(ii) organization reviews and approves the access list and authorization credentials in accordance with the organization-defined frequency; and
(iii) the organization removes from the access list personnel no longer requiring access.</td></tr>
<tr><td colspan="3"><b>Assessment Methods and Objects</b></td></tr>
<tr><td colspan="3"><b>Examine:</b> Physical and environmental protection policy; procedures addressing physical access authorizations; security plan; authorized personnel access list; authorization credentials; other relevant documents or records.</td></tr>
</table>

Table 152. PE-3: Physical Access Control

PE-3: Physical Access Control

Control

The organization:

a. Enforces physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides (excluding those areas within the facility officially designated as publicly accessible);

b. Verifies individual access authorizations before granting access to the facility;

c Controls entry to the facility containing the information system using physical access devices and/or guards;

d. Controls access to areas officially designated as publicly accessible in accordance with the organization's assessment of risk;

e. Secures keys, combinations, and other physical access devices;

f. Inventories physical access devices within every three hundred sixty-five (365) days; and

g. Changes combinations and keys when keys are lost, combinations are compromised, or individuals are transferred or terminated.

For FTI:

h. Minimum protection standards require two physical barriers between FTI and an individual not authorized to access FTI. This may be achieved through secured perimeter/locked container, locked perimeter/secured interior or locked perimeter/security container. FTI must be containerized in areas where other than authorized employees or authorized contractors may have access after-hours.

i. A security guard, custodial services worker or landlord may have access to a locked building or a locked room if FTI is in a locked container. If FTI is in a locked room, but not in a locked container, the guard, janitor or landlord may have a key to the building but not to the room.

j. During business hours, if authorized personnel serve as the second barrier between FTI and unauthorized individuals, the authorized personnel must wear an identification badge or credential clearly displayed, preferably work above the waist.

k. Unauthorized access to areas containing FTI during duty and non-duty hours must be denied. This can be done utilizing a combination of methods: secured or locked perimeter, secured area or containerization.

l. The physical security and control of computers and electronic media must be addressed. Computer operations must be in a secure area with restricted access.

Guidance

The organization determines the types of guards needed, for example, professional physical security staff or other personnel such as administrative staff or information system users, as deemed appropriate. Physical access devices include, for example, keys, locks, combinations, and card readers. Workstations and associated peripherals connected to (and part of) an organizational information system may be located in areas designated as publicly accessible with access to such devices being safeguarded.

Applicability: Exchanges	**Reference(s):** IRS-1075: 4.2, 4.3, 4.6	**Related Control Requirements:** MP-2, MP-4, PE-2

Assessment Procedure: PE-3.1

Assessment Objective

Determine if:

(i) the organization enforces physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides (excluding those areas within the facility officially designated as publicly accessible);

(ii) the organization verifies individual access authorizations before granting access to the facility;

(iii) the organization controls entry to the facility containing the information system using physical access devices (e.g., keys, locks, combinations, card readers) and/or guards;

(iv) the organization controls access to areas officially designated as publicly accessible in accordance with the organization’s assessment of risk; and

(v) the organization secures keys, combinations, and other physical access devices.

PE-3: Physical Access Control
Assessment Methods and Objects
Examine: Physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; information system entry and exit points; storage locations for physical access devices; other relevant documents or records.
Interview: Organizational personnel with physical access control responsibilities.
Assessment Procedure: PE-3.2
Assessment Objective
Determine if:
(i) the organization defines the frequency for conducting inventories of physical access devices; (ii) the organization inventories physical access devices in accordance with the organization-defined frequency; (iii) the organization defines the frequency of changes to combinations and keys; and (iv) the organization changes combinations and keys in accordance with the organization-defined frequency, and when keys are lost, combinations are compromised, or individuals are transferred or terminated.
Assessment Methods and Objects
Examine: Physical and environmental protection policy; procedures addressing physical access control; security plan; physical access control logs or records; inventory records of physical access devices; records of key and lock combination changes; storage locations for physical access devices; other relevant documents or records.

Table 153. PE-4: Access Control for Transmission Medium

<table>
<tr><th colspan="3">PE-4: Access Control for Transmission Medium</th></tr>
<tr><td colspan="3"><b>Control</b></td></tr>
<tr><td colspan="3">The organization controls physical access to information system distribution and transmission lines within organizational facilities.</td></tr>
<tr><td colspan="3"><b>Implementation Standards</b></td></tr>
<tr><td colspan="3">1. Permit access to telephone closets and information system distribution and transmission lines within organizational facilities only to authorized personnel.
2. Disable any physical ports (e.g., wiring closets, patch panels) not in use.</td></tr>
<tr><td colspan="3"><b>Guidance</b></td></tr>
<tr><td colspan="3">Physical protections applied to information system distribution and transmission lines help prevent accidental damage, disruption, and physical tampering. Additionally, physical protections are necessary to help prevent eavesdropping or in transit modification of unencrypted transmissions. Protective measures to control physical access to information system distribution and transmission lines include: (i) locked wiring closets; (ii) disconnected or locked spare jacks; and/or (iii) protection of cabling by conduit or cable trays.</td></tr>
<tr><td><b>Applicability:</b> Exchanges</td><td><b>Reference(s):</b> IRS-1075: 4.3.2</td><td><b>Related Control Requirements:</b> PE-2</td></tr>
<tr><td colspan="3"><b>Assessment Procedure: PE-4.1</b></td></tr>
<tr><td colspan="3"><b>Assessment Objective</b></td></tr>
<tr><td colspan="3">Determine if the organization controls physical access to information system distribution and transmission lines within organizational facilities.</td></tr>
<tr><td colspan="3"><b>Assessment Methods and Objects</b></td></tr>
<tr><td colspan="3"><b>Examine:</b> Physical and environmental protection policy; procedures addressing access control for transmission medium; information system design documentation; facility communications and wiring diagrams; other relevant documents or records.</td></tr>
</table>

Table 154Table 154. PE-5: Access Control for Output Devices

PE-5: Access Control for Output Devices		
Control		
The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output. For FTI: Output from printers and fax machines should be in a controlled area and secured when not in use. Physical access to monitors displaying FTI should be controlled to prevent unauthorized access to the display output.		
Guidance		
Monitors, printers, and audio devices are examples of information system output devices.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 4.3, 4.3.2	**Related Control Requirements:**
Assessment Procedure: PE-5.1		
Assessment Objective		
Determine if the organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.		
Assessment Methods and Objects		
Examine: Physical and environmental protection policy; procedures addressing access control for display medium; facility layout of information system components; actual displays from information system components; other relevant documents or records.		

Table 155. PE-6: Monitoring Physical Access

PE-6: Monitoring Physical Access		
Control		
The organization: a. Monitors physical access to the information system to detect and respond to physical security incidents; b. Reviews physical access logs in accordance with the frequency specified in Implementation Standard 1; and c. Coordinates results of reviews and investigations with the organization's incident response capability.		
Implementation Standard		
1. Review physical access logs every at least once every two (2) months.		
Guidance		
Investigation of and response to detected physical security incidents, including apparent security violations or suspicious physical access activities, are part of the organization’s incident response capability.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 4.3.2	**Related Control Requirements:**
Assessment Procedure: PE-6.1		
Assessment Objective		
Determine if:		
(i) the organization monitors physical access to the information system to detect and respond to physical security incidents; (ii) the organization defines the frequency to review physical access logs; (iii) the organization reviews physical access logs in accordance with the organization-defined frequency; and (iv) the organization coordinates results of reviews and investigations with the organization’s incident response capability.		

PE-6: Monitoring Physical Access		
Assessment Methods and Objects		
Examine: Physical and environmental protection policy; procedures addressing physical access monitoring; security plan; physical access logs or records; other relevant documents or records.		
Interview: Organizational personnel with physical access monitoring responsibilities.		

Table 156. PE-6(1): Monitoring Physical Access

PE-6(1): Monitoring Physical Access		
Control		
The organization monitors real-time physical intrusion alarms and surveillance equipment.		
Guidance		
Applicability: Exchanges	**Reference(s):**	**Related Control Requirements:**
Assessment Procedure: PE-6(1).1		
Assessment Objective		
Determine if the organization monitors real-time physical intrusion alarms and surveillance equipment.		
Assessment Methods and Objects		
Examine: Physical and environmental protection policy; procedures addressing physical access monitoring; physical intrusion alarm/surveillance equipment logs or records; other relevant documents or records.		
Interview: Organizational personnel with physical access monitoring responsibilities.		

Table 157. PE-7: Visitor Control

PE-7: Visitor Control		
Control		
The organization controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible. For FTI: A restricted area visitor log will be maintained at a designated entrance to the restricted area and all visitors (persons not assigned to the area) entering the area shall be directed to the designated entrance. The entry control monitor should verify the identity of visitors by comparing the name and signature entered into the register with some type of photo identification card.		
Guidance		
Individuals (to include organizational employees, contract personnel, and others) with permanent authorization credentials for the facility are not considered visitors.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 4.3.2	**Related Control Requirements:**
Assessment Procedure: PE-7.1		
Assessment Objective		
Determine if the organization controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible.		

PE-7: Visitor Control
Assessment Methods and Objects
Examine: Physical and environmental protection policy; procedures addressing visitor access control; visitor access control logs or records; other relevant documents or records.
Interview: Organizational personnel with visitor access control responsibilities.

Table 158. PE-7(1): Visitor Control

<table>
<tr><th colspan="3">PE-7(1): Visitor Control</th></tr>
<tr><td colspan="3"><b>Control</b></td></tr>
<tr><td colspan="3">The organization escorts visitors and monitors visitor activity, when required.</td></tr>
<tr><td colspan="3"><b>Guidance</b></td></tr>
<tr><td colspan="3"></td></tr>
<tr><td><b>Applicability:</b> Exchanges</td><td><b>Reference(s):</b> IRS-1075: 4.3.2</td><td><b>Related Control Requirements:</b></td></tr>
<tr><td colspan="3"><b>Assessment Procedure: PE-7(1).1</b></td></tr>
<tr><td colspan="3"><b>Assessment Objective</b></td></tr>
<tr><td colspan="3">Determine if the organization escorts visitors and monitors visitor activity, when required.</td></tr>
<tr><td colspan="3"><b>Assessment Methods and Objects</b></td></tr>
<tr><td colspan="3"><b>Examine:</b> Physical and environmental protection policy; procedures addressing visitor access control; visitor access control logs or records; other relevant documents or records.</td></tr>
<tr><td colspan="3"><b>Interview:</b> Organizational personnel with visitor access control responsibilities.</td></tr>
</table>

Table 159. PE-8: Access Records

<table>
<tr><th colspan="3">PE-8: Access Records</th></tr>
<tr><td colspan="3"><b>Control</b></td></tr>
<tr><td colspan="3">The organization:
a. Maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible); and
b. Reviews visitor access records monthly.
For FTI: The restricted area visitor log shall include the visitor’s name, signature, assigned work area, escort, purpose of entry, and time and date of entry.</td></tr>
<tr><td colspan="3"><b>Guidance</b></td></tr>
<tr><td colspan="3">Visitor access records include, for example, name/organization of the person visiting, signature of the visitor, form(s) of identification, date of access, time of entry and departure, purpose of visit, and name/organization of person visited.</td></tr>
<tr><td><b>Applicability:</b> Exchanges</td><td><b>Reference(s):</b> IRS-1075: 4.3.2</td><td><b>Related Control Requirements:</b></td></tr>
<tr><td colspan="3"><b>Assessment Procedure: PE-8.1</b></td></tr>
<tr><td colspan="3"><b>Assessment Objective</b></td></tr>
<tr><td colspan="3">Determine if:</td></tr>
<tr><td colspan="3">(i) the organization maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible);
(ii) the organization defines the frequency to review visitor access records;
(iii) the organization reviews the visitor access records in accordance with the organization-defined frequency.</td></tr>
<tr><td colspan="3"><b>Assessment Methods and Objects</b></td></tr>
</table>

PE-8: Access Records
Examine: Physical and environmental protection policy; procedures addressing facility access records; security plan; facility access control records; other relevant documents or records.
Interview: Organizational personnel with responsibilities for reviewing physical access records.

Table 160. PE-9: Power Equipment and Power Cabling

<table>
<tr><th colspan="3">PE-9: Power Equipment and Power Cabling</th></tr>
<tr><td colspan="3"><b>Control</b></td></tr>
<tr><td colspan="3">The organization protects power equipment and power cabling for the information system from damage and destruction.</td></tr>
<tr><td colspan="3"><b>Implementation Standard</b></td></tr>
<tr><td colspan="3">1. Permit only authorized maintenance personnel to access infrastructure assets, including power generators, HVAC systems, cabling, and wiring closets.</td></tr>
<tr><td colspan="3"><b>Guidance</b></td></tr>
<tr><td colspan="3">This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.</td></tr>
<tr><td><b>Applicability:</b>
Exchanges</td><td><b>Reference(s):</b></td><td><b>Related Control Requirements:</b></td></tr>
<tr><td colspan="3"><b>Assessment Procedure: PE-9.1</b></td></tr>
<tr><td colspan="3"><b>Assessment Objective</b></td></tr>
<tr><td colspan="3">Determine if the organization protects power equipment and power cabling for the information system from damage and destruction.</td></tr>
<tr><td colspan="3"><b>Assessment Methods and Objects</b></td></tr>
<tr><td colspan="3"><b>Examine:</b> Physical and environmental protection policy; procedures addressing power equipment and cabling protection; facility housing power equipment and cabling; other relevant documents or records.</td></tr>
</table>

Table 161. PE-10: Emergency Shutoff

<table>
<tr><th colspan="3">PE-10: Emergency Shutoff</th></tr>
<tr><td colspan="3"><b>Control</b></td></tr>
<tr><td colspan="3">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 a location that does not require personnel to approach the equipment to facilitate safe and easy access for personnel; and
c. Protects emergency power shutoff capability from unauthorized activation.</td></tr>
<tr><td colspan="3"><b>Guidance</b></td></tr>
<tr><td colspan="3">This control applies to facilities containing concentrations of information system resources, for example, data centers, server rooms, and mainframe computer rooms.</td></tr>
<tr><td><b>Applicability:</b>
Exchanges</td><td><b>Reference(s):</b></td><td><b>Related Control Requirements:</b></td></tr>
</table>

PE-10: Emergency Shutoff		
Assessment Procedure: PE-10.1		
Assessment Objective		
Determine if:		
(i) the organization provides the capability of shutting off power to the information system or individual system components in emergency situations; (ii) the organization defines the location of emergency shutoff switches or devices by information system or system component; (iii) the organization places emergency shutoff switches or devices in an organization-defined location by information system or system component to facilitate safe and easy access for personnel; and (iv) the organization protects the emergency power shutoff capability from unauthorized activation.		
Assessment Methods and Objects		
Examine: Physical and environmental protection policy; procedures addressing power source emergency shutoff; security plan; emergency shutoff controls or switches; other relevant documents or records.		

Table 162. PE-11: Emergency Power

PE-11: Emergency Power		
Control		
The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.		
Guidance		
This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.		
Applicability: Exchanges	**Reference(s):**	**Related Control Requirements:**
Assessment Procedure: PE-11.1		
Assessment Objective		
Determine if the organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.		
Assessment Methods and Objects		
Examine: Physical and environmental protection policy; procedures addressing emergency power; uninterruptible power supply documentation; uninterruptible power supply test records; other relevant documents or records.		

Table 163. PE-12: Emergency Lighting

PE-12: Emergency Lighting		
Control		
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.		
Guidance		
This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.		
Applicability: Exchanges	**Reference(s):**	**Related Control Requirements:**
Assessment Procedure: PE-12.1		

PE-12: Emergency Lighting
Assessment Objective
Determine if:
(i) the organization employs automatic emergency lighting for the information system that activates in the event of a power outage or disruption; (ii) the organization employs automatic emergency lighting for the information system that covers emergency exits and evacuation routes within the facility; and (iii) the organization maintains the automatic emergency lighting for the information system.
Assessment Methods and Objects
Examine: Physical and environmental protection policy; procedures addressing emergency lighting; emergency lighting documentation; emergency lighting test records; emergency exits and evacuation routes; other relevant documents or records.
Interview: Organizational personnel with emergency planning responsibilities.

Table 164. PE-13: Fire Protection

PE-13: Fire Protection		
Control		
The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.		
Guidance		
Fire suppression and detection devices/systems include, for example, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors. This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.		
Applicability: Exchanges	**Reference(s):**	**Related Control Requirements:**
Assessment Procedure: PE-13.1		
Assessment Objective		
Determine if:		
(i) the organization employs fire suppression and detection devices/systems for the information system that are supported by an independent energy source; and (ii) the organization maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.		
Assessment Methods and Objects		
Examine: Physical and environmental protection policy; procedures addressing fire protection; fire suppression and detection devices/systems; fire suppression and detection devices/systems documentation; test records of fire suppression and detection devices/systems; other relevant documents or records.		
Interview: Organizational personnel with responsibilities for fire detection and suppression devices/systems.		

Table 165. PE-13(1): Fire Protection

PE-13(1): Fire Protection
Control
The organization employs fire detection devices/systems for the information system that activate automatically and notify the organization and emergency responders in the event of a fire.
Guidance

PE-13(1): Fire Protection		
Applicability: Exchanges	**Reference(s):**	**Related Control Requirements:**
Assessment Procedure: PE-13(1).1		
Assessment Objective		
Determine if the organization employs fire detection devices/systems for the information system that, without manual intervention, activate automatically and notify the organization and emergency responders in the event of a fire.		
Assessment Methods and Objects		
Examine: Physical and environmental protection policy; procedures addressing fire protection; facility housing the information system; alarm service level agreements; test records of fire suppression and detection devices/systems; fire suppression and detection devices/systems documentation; other relevant documents or records.		
Interview: Organizational personnel with responsibilities for fire detection and suppression devices/systems.		

Table 166. PE-13(2): Fire Protection

PE-13(2): Fire Protection		
Control		
The organization employs fire suppression devices/systems for the information system that provide automatic notification of any activation to the organization and emergency responders.		
Guidance		
Applicability: Exchanges	**Reference(s):**	**Related Control Requirements:**
Assessment Procedure: PE-13(2).1		
Assessment Objective		
Determine if the organization employs fire suppression devices/systems for the information system that provide automatic notification of any activation to the organization and emergency responders.		
Assessment Methods and Objects		
Examine: Physical and environmental protection policy; procedures addressing fire protection; fire suppression and detection devices/systems documentation; facility housing the information system; alarm service level agreements; test records of fire suppression and detection devices/systems; other relevant documents or records.		
Interview: Organizational personnel with responsibilities for fire detection and suppression devices/systems.		

Table 167. PE-13(3): Fire Protection

PE-13(3): Fire Protection		
Control		
The organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.		
Guidance		
Applicability: Exchanges	**Reference(s):**	**Related Control Requirements:**
Assessment Procedure: PE-13(3).1		
Assessment Objective		
Determine if the organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.		

PE-13(3): Fire Protection
Assessment Methods and Objects
Examine: Physical and environmental protection policy; procedures addressing fire protection; facility housing the information system; alarm service level agreements; facility staffing plans; test records of fire suppression and detection devices/systems; other relevant documents or records.
Interview: Organizational personnel with responsibilities for fire detection and suppression devices/systems.

Table 168. PE-14: Temperature and Humidity Controls

PE-14: Temperature and Humidity Controls		
Control		
The organization: a. Maintains temperature and humidity levels within the facility where the information system resides within acceptable vendor-recommended levels; and b. Monitors temperature and humidity levels.		
Implementation Standards		
1. Evaluate the level of alert and follow prescribed guidelines for that alert level. 2. Alert component management of possible loss of service and/or media. 3. Report damage and provide remedial action. Implement contingency plan, if necessary.		
Guidance		
This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.		
Applicability: Exchanges	**Reference(s):**	**Related Control Requirements:**
Assessment Procedure: PE-14.1		
Assessment Objective		
Determine if:		
(i) the organization defines the acceptable temperature and humidity levels within the facility where the information system resides; (ii) the organization maintains temperature and humidity levels within the facility where the information system resides in accordance with organization-defined acceptable levels; (iii) the organization defines the frequency to monitor temperature and humidity levels; and (iv) the organization monitors the temperature and humidity levels within the facility where the information system resides in accordance with the organization-defined frequency.		
Assessment Methods and Objects		
Examine: Physical and environmental protection policy; procedures addressing temperature and humidity control; security plan; temperature and humidity controls; facility housing the information system; temperature and humidity controls documentation; temperature and humidity records; other relevant documents or records.		

Table 169. PE-15: Water Damage Protection

PE-15: Water Damage Protection		
Control		
The organization protects the information system from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.		
Guidance		
This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.		
Applicability: Exchanges	**Reference(s):**	**Related Control Requirements:**
Assessment Procedure: PE-15.1		
Assessment Objective		
Determine if:		
(i) the organization protects the information system from damage resulting from water leakage by providing master shutoff valves that are accessible and working properly; and (ii) key personnel within the organization have knowledge of the master water shutoff valves.		
Assessment Methods and Objects		
Examine: Physical and environmental protection policy; procedures addressing water damage protection; facility housing the information system; master shutoff valves; list of key personnel with knowledge of location and activation procedures for master shutoff valves for the plumbing system; master shutoff valve documentation; other relevant documents or records.		
Interview: Organization personnel with physical and environmental protection responsibilities.		

Table 170. PE-16: Delivery and Removal

PE-16: Delivery and Removal		
Control		
The organization authorizes, monitors, and controls the flow of information system-related components entering and exiting the facility and maintains records of those items. For FTI: All transportation or shipments of FTI (including electronic media or microfilm) must be documented on a transmittal form and monitored to ensure that each shipment is properly and timely received and acknowledged. All FTI transported through the mail or courier/messenger service must be double-sealed; that is one envelope within another envelope. The inner envelope should be marked confidential with some indication that only the designed official or delegate is authorized to open it.		
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.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 4.5	**Related Control Requirements:**
Assessment Procedure: PE-16.1		
Assessment Objective		
Determine if:		
(i) the organization defines the types of information system components to be authorized, monitored, and controlled as such components are entering or exiting the facility; (ii) the organization authorizes, monitors, and controls organization-defined information system components entering and exiting the facility; and (iii) the organization maintains records of information system components entering and exiting the facility.		

PE-16: Delivery and Removal
Assessment Methods and Objects
Examine: Physical and environmental protection policy; procedures addressing delivery and removal of information system components from the facility; security plan; facility housing the information system; records of items entering and exiting the facility; other relevant documents or records.
Interview: Organization personnel with responsibilities for controlling information system components entering and exiting the facility.

Table 171. PE-17: Alternate Work Site

PE-17: Alternate Work Site		
Control		
The organization: a. Employs appropriate security controls at alternate work sites to include, but not limited to, laptop cable locks, recording serial numbers and other identification information about laptops, and disconnecting modems; 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. For FTI: Describe the policies and procedures for meeting the minimum protection standards for alternative work sites (e.g. employee’s homes or other non-traditional work sites).		
Guidance		
Alternate work sites may include, for example, government facilities or private residences of employees. The organization may define different sets of security controls for specific alternate work sites or types of sites.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 5.3	**Related Control Requirements:**
Assessment Procedure: PE-17.1		
Assessment Objective		
Determine if:		
(i) the organization defines the management, operational, and technical information system security controls to be employed at alternate work sites; (ii) the organization employs organization-defined management, operational, and technical information system security controls at alternate work sites; (iii) the organization assesses, as feasible, the effectiveness of security controls at alternate work sites; and (iv) the organization provides a means for employees to communicate with information security personnel in case of security incidents or problems.		
Assessment Methods and Objects		
Examine: Physical and environmental protection policy; procedures addressing alternate work sites for organizational personnel; security plan; list of management, operational, and technical security controls required for alternate work sites; assessments of security controls at alternate work sites; other relevant documents or records.		
Interview: Organization personnel using alternate work sites.		

Table 172. PE-18: Location of Information System Components

<table>
<tr><th colspan="3">PE-18: Location of Information System Components</th></tr>
<tr><td colspan="3"><b>Control</b></td></tr>
<tr><td colspan="3">The organization positions information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.</td></tr>
<tr><td colspan="3"><b>Guidance</b></td></tr>
<tr><td colspan="3">Physical and environmental hazards include, for example, flooding, fire, tornados, earthquakes, hurricanes, acts of terrorism, vandalism, electromagnetic pulse, electrical interference, and electromagnetic radiation. Whenever possible, the organization also considers the location or site of the facility with regard to physical and environmental hazards. In addition, the organization considers the location of physical entry points where unauthorized individuals, while not being granted access, might nonetheless be in close proximity to the information system and therefore, increase the potential for unauthorized access to organizational communications (e.g., through the use of wireless sniffers or microphones). This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.</td></tr>
<tr><td><b>Applicability:</b> Exchanges</td><td><b>Reference(s):</b> IRS-1075: 4.3.2</td><td><b>Related Control Requirements:</b></td></tr>
<tr><td colspan="3"><b>Assessment Procedure: PE-18.1</b></td></tr>
<tr><td colspan="3"><b>Assessment Objective</b></td></tr>
<tr><td colspan="3">Determine if:</td></tr>
<tr><td colspan="3">(i) the organization positions information system components within the facility to minimize potential damage from physical and environmental hazards; and
(ii) the organization positions information system components within the facility to minimize the opportunity for unauthorized access.</td></tr>
<tr><td colspan="3"><b>Assessment Methods and Objects</b></td></tr>
<tr><td colspan="3"><b>Examine:</b> Physical and environmental protection policy; procedures addressing positioning of information system components; documentation providing the location and position of information system components within the facility; other relevant documents or records.</td></tr>
</table>

Planning (PL) – Operational

Table 173. PL-1: Security Planning Policy and Procedures

PL-1: Security Planning Policy and Procedures		
Control		
The organization develops, disseminates, and reviews/updates within every three-hundred-sixty-five (365) days: a. A formal, documented security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.		
Guidance		
This control is intended to produce the policy and procedures that are required for the effective implementation of security controls and control enhancements in the security planning family. The policy and procedures are consistent with CMS guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The security planning policy addresses the overall policy requirements for confidentiality, integrity, and availability and can be included as part of the general information security policy for the organization. Security planning procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the security planning policy.		
Applicability: Exchanges	**Reference(s):** HIPAA: 164.308(a)(1)(i), 164.316(a); HSPD 7: J(35); IRS-1075: 9.13	**Related Control Requirements:**
Assessment Procedure: PL-1.1		
Assessment Objective		
Determine if:		
(i) the organization develops and formally documents security planning policy; (ii) the organization security planning policy addresses: – purpose; – scope; – roles and responsibilities; – management commitment; – coordination among organizational entities; – compliance; (iii) the organization disseminates formal documented security planning policy to elements within the organization having associated security planning roles and responsibilities; (iv) the organization develops and formally documents security planning procedures; (v) the organization security planning procedures facilitate implementation of the security planning policy and associated security planning controls; (vi) the organization disseminates formal documented security planning procedures to elements within the organization having associated security planning roles and responsibilities; (vii) the organization reviews/updates the security planning policy and procedures within every three-hundred-sixty-five (365) days.		
Assessment Methods and Objects		
Examine: Security planning policy and procedures; other relevant documents or records.		
Interview: Organizational personnel with security planning responsibilities.		

Table 174. PL-2: System Security Plan (SSP)

PL-2: Security System Plan (SSP)

Control

The organization:

a. Develops a security plan for the information system that:
   - Is consistent with the ACA System Security Plan (SSP) Procedure;
   - Is consistent with the organization's enterprise architecture;
   - Explicitly defines the authorization boundary for the system;
   - Describes the operational context of the information system in terms of missions and business processes;
   - Describes the operational environment for the information system;
   - Describes relationships with or connections to other information systems;
   - Provides an overview of the security requirements for the system;
   - Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and
   - Is reviewed and approved by the authorizing official or designated representative prior to plan implementation;

b. Reviews the security plan for the information system within every three-hundred-sixty-five (365) days; and

c. Updates the plan, minimally every three (3) years, to address current conditions or whenever:
   - There are significant changes to the information system/environment of operation that affect security;
   - Problems are identified during plan implementation or security control assessments:
   - When the data sensitivity level increases;
   - After a serious security violation due to changes in the threat environment; or
   - Before the previous security authorization expires.

For FTI:

1. When FTI is incorporated into a Data Warehouse, the controls described in IRS Pub. 1075, Exhibit 11 are to be followed, in addition to those specified in other controls.
2. Develop and submit a Safeguard Procedures Report (SPR) that describes the procedures established and used by the organization for ensuring the confidentiality of the information received from the IRS. Annually thereafter, the organization must file a Safeguard Activity Report (SAR). The SAR advises the IRS of minor changes to the procedures or safeguards described in the SPR. It also advises the IRS of future actions that will affect the organization's safeguard procedures, summarizes the organization's current efforts to ensure the confidentiality of FTI, and finally, certifies that the organization is protecting FTI pursuant to IRC Section 6103(p)(4) and the organization's own security requirements. Whenever significant changes occur in the safeguard program, the SPR will be updated and resubmitted. (See IRS Pub. 1075, sections 7.0 and 9.13)

Implementation Standards

1. (For PHI only) Retain documentation of policies and procedures relating to HIPAA 164.306 for six (6) years from the date of its creation or the date when it last was in effect, whichever is later. [See HIPAA 164.316(b).]

Guidance

The security plan contains sufficient information (including specification of parameters for assignment and selection statements in security controls either explicitly or by reference) to enable an implementation that is unambiguously compliant with the intent of the plan and a subsequent determination of risk to operations and assets, individuals, other organizations, and the Nation if the plan is implemented as intended.

All ACA information systems and major applications are covered by an SSP, which is compliant with current ACA SSP Procedures.

Applicability: Exchanges	**Reference(s):** HIPAA: 164.316(a); HSPD 7: J(35); IRS-1075: 7.0, 9.13	**Related Control Requirements:**

PL-2: Security System Plan (SSP)
Assessment Procedure: PL-2.1
Assessment Objective
Determine if:
(i) the organization develops a security plan for the information system that: – is consistent with the organization's enterprise architecture; – explicitly defines the authorization boundary for the system; – describes the operational context of the information system in terms of mission and business processes; – describes the operational environment for the information system; – describes relationships with or connections to other information systems; – provides an overview of the security requirements for the system; – describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplemental decisions; – is reviewed and approved by the authorizing official or designated representative prior to plan implementation; (ii) the organization defines the frequency of security plan reviews; (iii) the organization reviews the security plan in accordance with the organization-defined frequency, minimally every three (3) years; (iv) the organization updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments. (v) the organization meets all the requirements specified in the applicable implementation standard(s).
Assessment Methods and Objects
Examine: Security planning policy; procedures addressing security plan development and implementation; procedures addressing security plan reviews and updates; enterprise architecture documentation; security plan for the information system; records of security plan reviews and updates; other relevant documents or records.
Examine: Sampling of policies and procedures relating to 164.306 for retention period. [See HIPAA 164.316(b).]
Examine: Compliance controls if FTI is incorporated into a Data Warehouse. (See IRS Pub 1075 Exhibit 7.)
Examine: SPRs and SARs
Examine: Procedures that document who obtains documentation and which documentation pertains to whom for implementation.
Interview: Organizational personnel with security planning and plan implementation responsibilities for the information system.
Interview: Organizational personnel with retention responsibilities related to 164.306. [See HIPAA 164.316(b).]
Interview: Organizational personnel who are responsible for implementation of procedures to determine if documentation is available.

Table 175. PL-4: Rules of Behavior

PL-4: Rules of Behavior		
Control		
The organization: a. Establishes and makes readily available to all information system users, the rules that describe their responsibilities and expected behavior with regard to information, information system, and network use; and b. Receives signed acknowledgment from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system.		
Guidance		
The organization considers different sets of rules based on user roles and responsibilities, for example, differentiating between the rules that apply to privileged users and rules that apply to general users. Electronic signatures are acceptable for use in acknowledging rules of behavior.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.13	**Related Control Requirements:** PS-6
Assessment Procedure: PL-4.1		

PL-4: Rules of Behavior
Assessment Objective
Determine if:
(i) the organization establishes the rules that describe information system user responsibilities and expected behavior with regard to information and information system usage; (ii) the organization makes the rules available to all information system users; and (iii) the organization receives a signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system.
Assessment Methods and Objects
Examine: Security planning policy; procedures addressing rules of behavior for information system users; rules of behavior; other relevant documents or records.
Interview: Organizational personnel who are authorized users of the information system and have signed rules of behavior.

Table 176. PL-5: Privacy Impact Assessment (PIA)

PL-5: Privacy Impact Assessment (PIA)		
Control		
The organization conducts a Privacy Impact Assessment (PIA) on the Exchange information system in accordance with OMB policy M-03-22.		
Applicability: Exchanges	**Reference(s):**	**Related Control Requirements:**
Assessment Procedure: PL-5.1		
Assessment Objective		
Determine if:		
(i) the organization conducts a privacy impact assessment on the information system; (ii) the privacy impact assessment is in accordance with OMB policy.		
Assessment Methods and Objects		
Examine: Security planning policy; procedures addressing privacy impact assessments on the information system; privacy impact assessment; other relevant documents or records.		

Table 177. PL-6: Security-Related Activity Planning

PL-6: Security-Related Activity Planning		
Control		
The organization plans and coordinates security-related activities affecting the information system before conducting such activities in order to reduce the impact on operations (i.e., mission, functions, image, and reputation), assets, and individuals.		
Guidance		
Security-related activities include, for example, security assessments, audits, system hardware and software maintenance, and contingency plan testing/exercises. Organizational advance planning and coordination includes both emergency and nonemergency (i.e., planned or non-urgent unplanned) situations.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.13	**Related Control Requirements:**

PL-6: Security-Related Activity Planning
Assessment Procedure: PL-6.1
Assessment Objective
Determine if the organization plans and coordinates security-related activities affecting the information system before conducting such activities in order to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation), organizational assets, and individuals.
Assessment Methods and Objects
Examine: Security planning policy; procedures addressing security-related activity planning for the information system; other relevant documents or records.
Interview: Organizational personnel with security planning and plan implementation responsibilities.

Personnel Security (PS) – Operational

Table 178. PS-1: Personnel Security Policy and Procedures

PS-1: Personnel Security Policy and Procedures		
Control		
The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days: a. A formal, documented personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.		
Guidance		
This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the personnel security family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The personnel security policy can be included as part of the general information security policy for the organization. Personnel security procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the personnel security policy.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.12	**Related Control Requirements:** PM-9
Assessment Procedure: PS-1.1		
Assessment Objective		
Determine if:		
(i) the organization develops and formally documents personnel security policy; (ii) the organization personnel security policy addresses: - purpose; - scope; - roles and responsibilities; - management commitment; - coordination among organizational entities; and - compliance; (iii) the organization disseminates formal documented personnel security policy to elements within the organization having associated personnel security roles and responsibilities; (iv) the organization develops and formally documents personnel security procedures; (v) the organization personnel security procedures facilitate implementation of the personnel security policy and associated personnel security controls; and (vi) the organization disseminates formal documented personnel security procedures to elements within the organization having associated personnel security roles and responsibilities.		
Assessment Methods and Objects		
Examine: Personnel security policy and procedures, other relevant documents or records.		
Interview: Organizational personnel with personnel security responsibilities.		
Assessment Procedure: PS-1.2		
Assessment Objective		
Determine if:		
(i) the organization defines the frequency of personnel security policy reviews/updates; (ii) the organization reviews/updates personnel security policy in accordance with organization-defined frequency; and (iii) the organization defines the frequency of personnel security procedure reviews/updates; (iv) the organization reviews/updates personnel security procedures in accordance with organization-defined frequency.		

<table>
<tr><th>PS-1: Personnel Security Policy and Procedures</th></tr>
<tr><td><b>Assessment Methods and Objects</b></td></tr>
<tr><td><b>Examine:</b> Personnel security policy and procedures, other relevant documents or records.</td></tr>
<tr><td><b>Interview:</b> Organizational personnel with personnel security responsibilities.</td></tr>
</table>

Table 179. PS-2: Position Categorization

<table>
<tr><th colspan="3">PS-2: Position Categorization</th></tr>
<tr><td colspan="3"><b>Control</b></td></tr>
<tr><td colspan="3">The organization:
a. Assigns a criticality/sensitivity risk designation to all positions;
b. Establishes screening criteria for individuals filling those positions; and
c. Reviews and revises position criticality/sensitivity risk designations within every three hundred sixty-five (365) days.</td></tr>
<tr><td colspan="3"><b>Guidance</b></td></tr>
<tr><td colspan="3">Position risk designations are consistent with Office of Personnel Management policy and guidance. The screening criteria include explicit information security role appointment requirements (e.g., training, security clearance).</td></tr>
<tr><td><b>Applicability:</b> Exchanges</td><td><b>Reference(s):</b> IRS-1075: 9.12</td><td><b>Related Control Requirements:</b></td></tr>
<tr><td colspan="3"><b>Assessment Procedure: PS2.1</b></td></tr>
<tr><td colspan="3"><b>Assessment Objective</b></td></tr>
<tr><td colspan="3">Determine if:</td></tr>
<tr><td colspan="3">(i) the organization assigns a risk designation to all positions within the organization;
(ii) the organization establishes a screening criteria for individuals filling organizational positions;
(iii) the organization defines the frequency of risk designation reviews and updates for organizational positions; and
(iv) the organization reviews and revises</td></tr>
<tr><td colspan="3"><b>Assessment Methods and Objects</b></td></tr>
<tr><td colspan="3"><b>Examine:</b> Personnel security policy; procedures addressing position categorization; appropriate codes of federal regulations; list of risk designations for organizational positions; security plan; records of risk designation reviews and updates; other relevant documents or records.</td></tr>
<tr><td colspan="3"><b>Interview:</b> Organizational personnel with personnel security responsibilities.</td></tr>
</table>

Table 180. PS-3: Personnel Screening

<table>
<tr><th>PS-3: Personnel Screening</th></tr>
<tr><td><b>Control</b></td></tr>
<tr><td>The organization:
a. Screens individuals prior to authorizing access to the information system; and
b. Rescreens individuals periodically, consistent with the criticality/sensitivity rating of the position.
For FTI: Individuals must be screened before authorizing access to information systems and devices containing FTI.</td></tr>
<tr><td><b>Implementation Standards</b></td></tr>
<tr><td>1. Perform criminal history check for all persons prior to employment.
2. Require appropriate personnel to obtain and hold a moderate-risk security clearance as defined in the DHHS Personnel Security/Suitability Handbook.</td></tr>
<tr><td><b>Guidance</b></td></tr>
<tr><td>Screening and rescreening are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidance, and the criteria established for the risk designation of the assigned position. The</td></tr>
</table>

PS-3: Personnel Screening		
organization may define different rescreening conditions and frequencies for personnel accessing the information system based on the type of information processed, stored, or transmitted by the system.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.12	**Related Control Requirements:**
Assessment Procedure: PS-3.1		
Assessment Objective		
Determine if:		
(i) the organization screens individuals prior to authorizing access to the information system; (ii) the organization defines conditions requiring re-screening and, where re-screening is so indicated, the frequency of such re-screening; and (iii) the organization re-screens individuals according to organization-defined conditions requiring re-screening and, where re-screening is so indicated, the organization-defined frequency of such re-screening.		
Assessment Methods and Objects		
Examine: Personnel security policy; procedures addressing personnel screening; records of screened personnel; security plan; other relevant documents or records.		
Interview: Organizational personnel with personnel security responsibilities.		

Table 181. PS-4: Personnel Termination

PS-4: Personnel Termination		
Control		
The organization, upon termination of individual employment: a. Revokes system and physical access immediately following employee termination; b. Conducts exit interviews; c. Retrieves all security-related information system-related property; d. Retains access to information and information systems formerly controlled by terminated individual; and e. Immediately escorts employees terminated for cause out of the organization.		
Implementation Standards		
1. System access must be revoked prior to or during the employee termination process.		
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 individuals understand any security constraints imposed by being former employees and that proper accountability is achieved for all information system-related property. Exit interviews may not be possible for some employees (e.g., in the case of job abandonment, some illnesses, and non-availability of supervisors). Exit interviews are important for individuals with security clearances. Timely execution of this control is particularly essential for employees or contractors terminated for cause.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.12	**Related Control Requirements:**
Assessment Procedure: PS-4.1		
Assessment Objective		
Determine if:		
(i) the organization terminates information system access upon termination of individual employment; (ii) the organization conducts exit interviews of terminated personnel; (iii) the organization retrieves all security-related organizational information system related property from terminated personnel; and (iv) the organization retains access to organizational information and information systems formerly controlled by terminated personnel.		

PS-4: Personnel Termination
Assessment Methods and Objects
Examine: Personnel security policy; procedures addressing personnel termination; records of personnel termination actions; list of information system accounts; other relevant documents or records.
Interview: Organizational personnel with personnel security responsibilities.

Table 182. PS-5: Personnel Transfer

PS-5: Personnel Transfer		
Control		
The organization reviews logical and physical access authorizations to information systems/facilities when personnel are reassigned or transferred to other positions within the organization and initiates the following transfer or reassignment actions during the formal transfer process: a. Re-issuing appropriate information system-related property (e.g., keys, identification cards, building passes); b. Notification to security management; c. Closing obsolete accounts and establishing new accounts; and d. Revocation of all system access privileges (if applicable).		
Guidance		
This control applies when the reassignment or transfer of an employee is permanent or of such an extended duration as to make the actions warranted. In addition the organization defines the actions appropriate for the type of reassignment or transfer; whether permanent or temporary. Actions that may be required when personnel are transferred or reassigned to other positions within the organization include, for example: (i) returning old and issuing new keys, identification cards, and building passes; (ii) closing previous information system accounts and establishing new accounts; (iii) changing information system access authorizations; and (iv) providing for access to official records to which the employee had access at the previous work location and in the previous information system accounts.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.12	**Related Control Requirements:**
Assessment Procedure: PS-5.1		
Assessment Objective		
Determine if:		
(i) the organization reviews logical and physical access authorizations to information systems/facilities when personnel are reassigned or transferred to other positions within the organization; (ii) the organization defines the transfer or reassignment actions and the time period within which the actions must occur following formal transfer or reassignment; and (iii) the organization initiates the organization-defined transfer or reassignment actions within an organization-defined time period following formal transfer or reassignment.		
Assessment Methods and Objects		
Examine: Personnel security policy; procedures addressing personnel transfer; security plan; records of personnel transfer actions; list of information system and facility access authorizations; other relevant documents or records.		
Interview: Organizational personnel with personnel security responsibilities.		

Table 183. PS-6: Access Agreements

PS-6: Access Agreements
Control
The organization: a. Ensures that individuals requiring access to information or information systems sign appropriate access agreements prior to being granted access; and

PS-6: Access Agreements		
b. Reviews/updates the access agreements as part of the system security authorization or when a contract is renewed or extended. For FTI: Agencies must review information system access authorizations and initiate appropriate actions when personnel are reassigned or transferred to other positions within the organization.		
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 the information system to which access is authorized. Electronic signatures are acceptable for use in acknowledging access agreements unless specifically prohibited by organizational policy.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.12	**Related Control Requirements:** PL-4
Assessment Procedure: PS-6.1		
Assessment Objective		
Determine if:		
(i) the organization identifies appropriate access agreements for individuals requiring access to organizational information and information systems; (ii) individuals requiring access to organizational information and information systems sign appropriate access agreements prior to being granted access; (iii) the organization defines the frequency of reviews/updates for access agreements; and (iv) the organization reviews/updates the access agreements in accordance with the organization-defined frequency.		
Assessment Methods and Objects		
Examine: Personnel security policy; procedures addressing access agreements for organizational information and information systems; access agreements; access authorizations; personnel security criteria; other relevant documents or records.		
Interview: Organizational personnel with personnel security responsibilities.		

Table 184. PS-7: Third-Party Personnel Security

PS-7: Third-Party Personnel Security		
Control		
The organization: a. Establishes personnel security requirements including security roles and responsibilities for third-party providers; b. Documents personnel security requirements; and c. Monitors provider compliance.		
Implementation Standards		
1. Regulate the access provided to contractors and define security requirements for contractors. Contractors must be provided with minimal system and physical access, and must agree to and support the information security requirements. The contractor selection process must assess the contractor's ability to adhere to and support information security policies and standards.		
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. The organization explicitly includes personnel security requirements in acquisition-related documents.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.12	**Related Control Requirements:**
Assessment Procedure: PS-7.1		

PS-7: Third-Party Personnel Security
Assessment Objective
Determine if:
(i) the organization establishes personnel security requirements, including security roles and responsibilities, for third-party providers (ii) the organization documents personnel security requirements for third-party providers; and (iii) the organization monitors third-party provider compliance with personnel security requirements.
Assessment Methods and Objects
Examine: Personnel security policy; procedures addressing third-party personnel security; list of personnel security requirements; acquisition documents; compliance monitoring process; other relevant documents or records.
Interview: Organizational personnel with personnel security responsibilities; third-party providers.

Table 185. PS-8: Personnel Sanctions

PS-8: Personnel Sanctions		
Control		
The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.		
Guidance		
The sanctions process is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. The process is described in access agreements and can be included as part of the general personnel policies and procedures for the organization.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.12	**Related Control Requirements:** PL-4, PS-6
Assessment Procedure: PS-8.1		
Assessment Objective		
Determine if the organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.		
Assessment Methods and Objects		
Examine: Personnel security policy; procedures addressing personnel sanctions; rules of behavior; records of formal sanctions; other relevant documents or records.		
Interview: Organizational personnel with personnel security responsibilities.		

Risk Assessment (RA) – Management

Table 186. RA-1: Risk Assessment Policy and Procedures

RA-1: Risk Assessment Policy and Procedures		
Control		
The organization develops, disseminates, and reviews/updates within every three-hundred-sixty-five (365) days: a. A formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.		
Guidance		
This control is intended to produce the policy and procedures that are required for the effective implementation of security controls and control enhancements in the risk assessment family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The risk assessment policy can be included as part of the general information security policy for the organization. Risk assessment procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the risk assessment policy.		
Applicability: Exchanges	**Reference(s):** HIPAA: 164.306(a)(2), 164.316(a); IRS-1075: 9.14	**Related Control Requirements:**
Assessment Procedure: RA-1.1		
Assessment Objective		
Determine if:		
(i) the organization develops and formally documents risk assessment policy; (ii) the organization risk assessment policy addresses: – purpose; – scope; – roles and responsibilities; – management commitment; – coordination among organizational entities; – compliance; (iii) the organization disseminates formal documented risk assessment policy to elements within the organization having associated risk assessment roles and responsibilities; (iv) the organization develops and formally documents risk assessment procedures; (v) the organization risk assessment procedures facilitate implementation of the risk assessment policy and associated risk assessment controls; (vi) the organization disseminates formal documented risk assessment procedures to elements within the organization having associated risk assessment roles and responsibilities; (vii) the organization reviews/updates the risk assessment policy and procedures within every three-hundred-sixty-five (365) days.		
Assessment Methods and Objects		
Examine: Risk assessment policy and procedures; other relevant documents or records.		
Interview: Organizational personnel with risk assessment responsibilities.		

Table 187. RA-2: Security Categorization

RA-2: Security Categorization		
Control		
The organization: a. Categorizes information and the information system in accordance with applicable federal standards and guidance; b. Documents the security categorization results (including supporting rationale) in the security plan for the information system ; and c. Ensures the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.		
Guidance		
A clearly defined authorization boundary is a prerequisite for an effective security categorization. Security categorization describes the potential adverse impacts to organizational operations, assets, and individuals should the information and information system be comprised through a loss of confidentiality, integrity, or availability. The organization conducts the security categorization process as an organization-wide activity with the involvement of the CIO, CISO, Business Owner, senior information security officer, and information owners/stewards. The security categorization process facilitates the creation of an inventory of information assets, and in conjunction with CM-8, a mapping to the information system components where the information is processed, stored, and transmitted. All information systems categorized as High or Moderate are considered sensitive or to contain sensitive information (such as FTI or Privacy Act protected information). All information systems categorized as Low are considered non-sensitive or to contain non-sensitive information. Organizations implement the minimum security requirements and controls as established in the current *Minimum Acceptable Risk Standards for Exchanges – Exchange Reference Architecture Supplement* based on the system security categorization.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.14	**Related Control Requirements:** MP-4, SC-7
Assessment Procedure: RA-2.1		
Assessment Objective		
Determine if:		
(i) the organization categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; (ii) the organization documents the security categorization results (including supporting rationale) in the security plan for the information system; (iii) the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.		
Assessment Methods and Objects		
Examine: Risk assessment policy; procedures addressing security categorization of organizational information and information systems; security planning policy and procedures; security plan; security categorization documentation; other relevant documents or records.		
Interview: Organizational personnel with security categorization and risk assessment responsibilities.		

Table 188. RA-3: Risk Assessment

RA-3: Risk Assessment
Control
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; c. Reviews risk assessment results within every three-hundred-sixty-five (365) days; and d. Updates the risk assessment within every three (3) years or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and

RA-3: Risk Assessment

vulnerabilities), or other conditions that may impact the security or authorization state of the system.

Guidance

A clearly defined authorization boundary is a prerequisite for an effective risk assessment. Risk assessments take into account vulnerabilities, threat sources, and security controls planned or in place to determine the level of residual risk posed to organizational operations and assets, individuals, other organizations, and the Nation based on the operation of the information system. Risk assessments also take into account risk posed to organizational operations, assets, or individuals from external parties (e.g., service providers, contractors operating information systems on behalf of the organization, individuals accessing information systems, outsourcing entities).

Risk assessments can be conducted by organizations at various steps in the Risk Management Framework including: information system categorization; security control selection; security control implementation; security control assessment; information system authorization; and security control monitoring. RA-3 is a noteworthy security control 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 the security control selection process during the application of tailoring guidance for security control baselines and when considering supplementing the baselines with additional security controls or control enhancements.

Applicability: Exchanges	**Reference(s):** HIPAA: 164.306(a)(2), 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.316(a); HSPD 7: D(8), F(19); IRS-1075: 9.14	**Related Control Requirements:**

Assessment Procedure: RA-3.1

Assessment Objective

Determine if:

(i) the organization conducts an assessment of risk of the information system and the information it processes, stores, or transmits that includes the likelihood and magnitude of harm, from the unauthorized:
- access;
- use;
- disclosure;
- disruption;
- modification; or
- destruction;

(ii) the organization documents risk assessment results;

(iii) the organization reviews risk assessment results within every three-hundred-sixty-five (365) days;

(iv) the organization updates the risk assessment within every three (3) years 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 or authorization state of the system.

Assessment Methods and Objects

Examine: Risk assessment policy; security planning policy and procedures; procedures addressing organizational assessments of risk; security plan; risk assessment; other relevant documents or records.

Interview: Organizational personnel with risk assessment responsibilities.

Table 189. RA-5: Vulnerability Scanning

RA-5: Vulnerability Scanning

Control

The organization:

a. Scans for vulnerabilities in the information system and hosted applications within every ninety (90) days and when new vulnerabilities potentially affecting the system/applications are identified and reported;

b. Employs vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for:
   - Enumerating platforms, software flaws, and improper configurations;
   - Formatting and making transparent, checklists and test procedures; and
   - Measuring vulnerability impact;

c. Analyzes vulnerability scan reports and results from security control assessments;

d. Remediates legitimate vulnerabilities based on the Business Owner's risk prioritization in accordance with an organizational assessment of risk; and

d. Shares information obtained from the vulnerability scanning process and security control assessments with designated personnel throughout the organization on a "need to know" basis to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

For FTI: At a minimum, systems containing FTI shall be scanned quarterly to identify any vulnerability in the information system.

Implementation Standards

1. Perform external network penetration testing and conduct enterprise security posture review as needed but no less than once within every three-hundred-sixty-five (365) days, in accordance with organizational IS procedures.

Guidance

The security categorization of the information system guides the frequency and comprehensiveness of the vulnerability scans. Vulnerability analysis for custom software and applications may require additional, more specialized techniques and approaches (e.g., web-based application scanners, source code reviews, source code analyzers). Vulnerability scanning includes scanning for specific functions, ports, protocols, and services that should not be accessible to users or devices and for improperly configured or incorrectly operating information flow mechanisms. The organization considers using tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and that use the Open Vulnerability Assessment Language (OVAL) to test for the presence of vulnerabilities. The Common Weakness Enumeration (CWE) and the National Vulnerability Database (NVD) are also excellent sources for vulnerability information. In addition, security control assessments such as red team exercises are another source of potential vulnerabilities for which to scan.

Applicability: Exchanges	**Reference(s):** HIPAA: 164.306(a)(2); HSPD 7: F(19), G(24); IRS-1075: 9.14	**Related Control Requirements:**

Assessment Procedure: RA-5.1

Assessment Objective

Determine if:

(i) the organization employs vulnerability scanning tools and techniques that use standards to promote interoperability among tools and automate parts of the vulnerability management process that focus on:
   - enumerating platforms, software flaws, and improper configurations;
   - formatting/and making transparent checklists and test procedures;
   - measuring vulnerability impact;

(ii) the organization analyzes vulnerability scan reports and results from security control assessments;

(iii) the organization remediates legitimate vulnerabilities based on the Business Owner's risk prioritization in accordance with an organizational assessment of risk;

(iv) the organization shares information obtained from the vulnerability scanning process and security control assessments with designated personnel throughout the organization to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

(v) the organization meets all the requirements specified in the applicable implementation standard(s).

RA-5: Vulnerability Scanning
Assessment Methods and Objects
Examine: Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; security plan; vulnerability scanning results; patch and vulnerability management records; other relevant documents or records.
Interview: Organizational personnel with risk assessment and vulnerability scanning responsibilities.

Table 190. RA-5(1): Scanning Tools Update

RA-5(1): Scanning Tools Update		
Control		
The organization employs vulnerability scanning tools that include the capability to readily update the list of information system vulnerabilities scanned.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.14	**Related Control Requirements:**
Assessment Procedure: RA-5(1).1		
Assessment Objective		
Determine if the organization uses vulnerability scanning tools that have the capability to readily update the list of information system vulnerabilities scanned.		
Assessment Methods and Objects		
Examine: Risk assessment policy; procedures addressing vulnerability scanning; vulnerability scanning tools and techniques documentation; records of updates to vulnerabilities scanned; other relevant documents or records.		

System and Services Acquisition (SA) – Management

Table 191. SA-1: System and Services Acquisition Policy and Procedures

SA-1: System and Services Acquisition Policy and Procedures		
Control		
The organization develops, disseminates, and reviews/updates within every three-hundred-sixty-five (365) days: a. A formal, documented system and services acquisition policy that includes information security considerations and that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.		
Implementation Standards		
Guidance		
This control is intended to produce the policy and procedures that are required for the effective implementation of security controls and control enhancements in the system and services acquisition family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The system and services acquisition policy can be included as part of the general information security policy for the organization. System and services acquisition procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the system and services acquisition policy.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.15	**Related Control Requirements:** PM-9
Assessment Procedure: SA-1.1		
Assessment Objective		
Determine if:		
(i) the organization develops and formally documents system services and acquisition policy; (ii) the organization system services and acquisition policy addresses: – purpose; – scope; – roles and responsibilities; – management commitment; – coordination among organizational entities; – compliance; (iii) the organization disseminates formal documented system services and acquisition policy to elements within the organization having associated system services and acquisition roles and responsibilities; (iv) the organization develops and formally documents system services and acquisition procedures; (v) the organization system services and acquisition procedures facilitate implementation of the system and services acquisition policy and associated system services and acquisition controls; (vi) the organization disseminates formal documented system services and acquisition procedures to elements within the organization having associated system services and acquisition roles and responsibilities; (vii) the organization reviews/updates the system services and acquisition policy and procedures within every three-hundred-sixty-five (365) days. (viii) the organization meets all the requirements specified in the applicable implementation standard(s).		
Assessment Methods and Objects		
Examine: System and services acquisition policy and procedures; other relevant documents or records.		
Examine: Organizational documentation that contains the development, dissemination, and review/updates to FTI IRS documents received.		
Interview: Organizational personnel with system and services acquisition responsibilities.		

Table 192. SA-2: Allocation of Resources

<table>
<tr><th colspan="3">SA-2: Allocation of Resources</th></tr>
<tr><td colspan="3"><b>Control</b></td></tr>
<tr><td colspan="3">The organization:
a. Includes a determination of information security requirements for the information system in mission/business process planning;
b. Determines, documents, and allocates the resources required to protect the information system as part of its capital planning and investment control process;
c. Includes information security requirements in mission/business case planning, and
d. Establishes a discrete line item in programming and budgeting documentation for the implementation and management of information systems security.</td></tr>
<tr><td colspan="3"><b>Guidance</b></td></tr>
<tr><td colspan="3"></td></tr>
<tr><td><b>Applicability:</b> Exchanges</td><td><b>Reference(s):</b> IRS-1075: 9.15</td><td><b>Related Control Requirements:</b> PM-3, PM-11</td></tr>
<tr><td colspan="3"><b>Assessment Procedure: SA-2.1</b></td></tr>
<tr><td colspan="3"><b>Assessment Objective</b></td></tr>
<tr><td colspan="3">Determine if:</td></tr>
<tr><td colspan="3">(i) the organization includes a determination of the information security requirements for the information system in mission/business process planning;
(ii) the organization determines, documents, and allocates the resources required to protect the information system as part of its capital planning and investment control process; and
(iii) the organization establishes a discrete line item for information security in organizational programming and budgeting documentation.</td></tr>
<tr><td colspan="3"><b>Assessment Methods and Objects</b></td></tr>
<tr><td colspan="3"><b>Examine:</b> System and services acquisition policy; procedures addressing the allocation of resources to information security requirements; organizational programming and budgeting documentation; other relevant documents or records.</td></tr>
<tr><td colspan="3"><b>Interview:</b> Organizational personnel with capital planning and investment responsibilities.</td></tr>
</table>

Table 193. SA-3: Life Cycle Support

<table>
<tr><th colspan="3">SA-3: Life Cycle Support</th></tr>
<tr><td colspan="3"><b>Control</b></td></tr>
<tr><td colspan="3">The organization:
a. Manages the information system using the information security steps provided in the Exchange Life Cycle (See <i>Collaborative Environment and Governance Approach – Exchange Reference Architecture Supplement</i>);
b. Defines and documents information system security roles and responsibilities throughout the system development life cycle; and
c. Identifies individuals having information system security roles and responsibilities.</td></tr>
<tr><td><b>Applicability:</b> Exchanges</td><td><b>Reference(s):</b> IRS-1075: 9.15</td><td><b>Related Control Requirements:</b></td></tr>
<tr><td colspan="3"><b>Assessment Procedure: SA-3.1</b></td></tr>
<tr><td colspan="3"><b>Assessment Objective</b></td></tr>
<tr><td colspan="3">Determine if:</td></tr>
<tr><td colspan="3">(i) the organization manages the information system using the information security steps provided in the Exchange Life Cycle (See <i>Collaborative Environment and Governance Approach – Exchange Reference Architecture Supplement</i>);</td></tr>
</table>

SA-3: Life Cycle Support
(ii) the organization defines and documents information system security roles and responsibilities throughout the system development life cycle; (iii) the organization identifies individuals having information system security roles and responsibilities.
Assessment Methods and Objects
Examine: System and services acquisition policy; procedures addressing the integration of information security into the system development life cycle process; information system development life cycle documentation; other relevant documents or records.
Interview: Organizational personnel with information security and system life cycle development responsibilities.

Table 194. SA-4: Acquisition

SA-4: Acquisition
Control
The organization includes the following requirements and/or specifications, explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards: a. Security functional requirements/specifications; b. Security-related documentation requirements; and c. Developmental and evaluation-related assurance requirements.
Implementation Standards
1. Each contract and Statement of Work (SOW) that requires development or access to ACA information must include language requiring adherence to organizational security policies and standards, define security roles and responsibilities, and receive approval from organization officials. For FTI: 1. Whenever information systems contain FTI, the agency shall include security requirements and/or security specifications, either explicitly or by reference, in information system acquisition contracts based on an assessment of risk. The contract for the acquisition must contain Exhibit 7 language. 2. Agencies using a consolidated data center must implement appropriate controls to ensure the protection of FTI, including a Service Level Agreement (SLA) between the agency authorized to receive FTI and the data center.
Guidance
The acquisition documents for information systems, nformation system components, and information system services include, either explicitly or by reference, security requirements that describe: (i) required security capabilities (i.e., security needs and, as necessary, specific security controls and other specific applicable requirements); (ii) required design and development processes; (iii) required test and evaluation procedures; and (iv) required documentation. Solicitation Documents: Solicitation documents (e.g., Request for Proposal) for any information system shall include, either explicitly or by reference, security requirements that describe the required: (i) Security capabilities; (ii) Design and development processes; (iii) Test and evaluation procedures; and (iv) Documentation. The requirements in the solicitation documents shall permit updating security controls as new threats/vulnerabilities are identified and as new technologies are implemented. Use of Evaluated and Validated Products: For acquisition of security and security-enabled commercial-off-the-shelf (COTS) information technology products, when multiple products meet organizational requirements, preference shall be given to products that have been evaluated and validated through one or more of the following sources: 1. The National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation

SA-4: Acquisition		
Scheme; 2. The International Common Criteria Recognition Arrangements; and 3. The NIST Cryptographic Module Validation Program.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 5.5.2, 9.15	**Related Control Requirements:**
Assessment Procedure: SA-4.1		
Assessment Objective		
Determine if:		
(i) the organization includes the following requirements and/or specifications, explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards: – security functional requirements/specifications; – security-related documentation requirements; – developmental and evaluation-related assurance requirements. (ii) the organization meets all the requirements specified in the applicable implementation standard(s).		
Assessment Methods and Objects		
Examine: System and services acquisition policy; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; acquisition contracts for information systems or services; other relevant documents or records.		
Interview: Organizational personnel with information system security, acquisition, and contracting responsibilities.		

Table 195. SA-4(1): Acquisitions

SA-4(1): Acquisitions		
Control		
The organization requires in acquisition documents that vendors/contractors provide information describing the functional properties of the security controls to be employed within the information system, information system components, or information system services in sufficient detail to permit analysis and testing of the controls.		
Guidance		
Applicability: Exchanges	**Reference(s):**	**Related Control Requirements:**
Assessment Procedure: SA-4(1).1		
Assessment Objective		
Determine if the organization requires in acquisition documents that vendors/contractors provide information describing in the functional properties of the security controls to be employed within the information system, information system components, or information system services in sufficient detail to permit analysis and testing of the controls.		
Assessment Methods and Objects		
Examine: System and services acquisition policy; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; solicitation documents; acquisition documentation; acquisition contracts for information systems or services; other relevant documents or records.		

Table 196. SA-4(4): Acquisitions

SA-4(4): Acquisitions		
Control		
The organization ensures that each information system component acquired is explicitly assigned to an information system, and that the owner of the system acknowledges this assignment.		
Guidance		
Applicability: Exchanges	**Reference(s):**	**Related Control Requirements:**
Assessment Procedure: SA-4(4).1		
Assessment Objective		
(i) the organization explicitly assigns each acquired information system component to an information system; and (ii) the owner of the system acknowledges each assignment of information system components to the information system.		
Assessment Methods and Objects		
Examine: System and services acquisition policy; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; solicitation documents; acquisition documentation; acquisition contracts for information systems or services; other relevant documents or records.		
Interview: Organizational personnel with information system security, acquisition, and contracting responsibilities; information system owner.		

Table 197. SA-5: Information System Documentation

SA-5: Information System Documentation
Control
The organization: a. Obtains, protects as required, and makes available to authorized personnel, administrator documentation for the information system that describes: – Secure configuration, installation, and operation of the information system; – Effective use and maintenance of security features/functions; and – Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions; and c. Obtains, protects as required, and makes available to authorized personnel, user documentation for the information system that describes: – User-accessible security features/functions and how to effectively use those security features/functions; – Methods for user interaction with the information system, which enables individuals to use the system in a more secure manner; and – User responsibilities in maintaining the security of the information and information system; and d. Documents attempts to obtain information system documentation when such documentation is either unavailable or nonexistent.
Implementation Standards
1. Develop system documentation to describe the system and to specify the purpose, technical operation, access, maintenance, and required training for administrators and users. 2. Maintain an updated list of related system operations and security documentation. 3. Update documentation upon changes in system functions and processes. Must include date and version number on all formal system documentation.

SA-5: Information System Documentation		
Guidance		
The inability of the organization to obtain necessary information system documentation may occur, for example, due to the age of the system and/or lack of support from the vendor/contractor. In those situations, organizations may need to recreate selected information system documentation if such documentation is essential to the effective implementation and/or operation of security controls.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.15	**Related Control Requirements:**
Assessment Procedure: SA-5.1		
Assessment Objective		
Determine if:		
(i) the organization obtains, protects as required, and makes available to authorized personnel, administrator documentation for the information system that describes: – secure configuration, installation, and operation of the information system; – effective use and maintenance of the security features/functions; and – known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions; (ii) the organization obtains, protects as required, and makes available to authorized personnel, user documentation for the information system that describes: – user-accessible security features/functions and how to effectively use those security features/functions; – methods for user interaction with the information system, which enables individuals to use the system in a more secure manner; and – user responsibilities in maintaining the security of the information and information system; and (iii) the organization documents attempts to obtain information system documentation when such documentation is either unavailable or nonexistent.		
Assessment Methods and Objects		
Examine: System and services acquisition policy; procedures addressing information system documentation; information system documentation including administrator and user guides; records documenting attempts to obtain unavailable or nonexistent information system documentation; other relevant documents or records.		
Interview: Organizational personnel with information system documentation responsibilities; organizational personnel operating, using, and/or maintaining the information system.		

Table 198. SA-5(1): Information System Documentation

SA-5(1): Information System Documentation		
Control		
The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing.		
Guidance		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.15	**Related Control Requirements:**
Assessment Procedure: SA-5(1).1		
Assessment Objective		
Determine if the organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing.		

SA-5(1): Information System Documentation
Assessment Methods and Objects
Examine: System and services acquisition policy; procedures addressing information system documentation; information system design documentation; other relevant documents or records.
Interview: Organizational personnel with information system security, acquisition, and contracting responsibilities; organizational personnel operating, using, and/or maintaining the information system.

Table 199. SA-5(3): Information System Documentation

<table>
<tr><th colspan="3">SA-5(3): Information System Documentation</th></tr>
<tr><td colspan="3"><b>Control</b></td></tr>
<tr><td colspan="3">The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the high-level design of the information system in terms of subsystems and implementation details of the security controls employed within the system with sufficient detail to permit analysis and testing.</td></tr>
<tr><td colspan="3"><b>Guidance</b></td></tr>
<tr><td colspan="3">An information system can be partitioned into multiple subsystems.</td></tr>
<tr><td><b>Applicability:</b> Exchanges</td><td><b>Reference(s):</b> IRS-1075: 9.15</td><td><b>Related Control Requirements:</b></td></tr>
<tr><td colspan="3"><b>Assessment Procedure: SA-5(3).1</b></td></tr>
<tr><td colspan="3"><b>Assessment Objective</b></td></tr>
<tr><td colspan="3"></td></tr>
<tr><td colspan="3"><b>Assessment Methods and Objects</b></td></tr>
<tr><td colspan="3"><b>Examine:</b> System and services acquisition policy; procedures addressing information system documentation; information system design documentation; other relevant documents or records.</td></tr>
<tr><td colspan="3"><b>Interview:</b> Organizational personnel with information system security, acquisition, and contracting responsibilities; organizational personnel operating, using, and/or maintaining the information system.</td></tr>
</table>

Table 200. SA-6: Software Usage Restrictions

<table>
<tr><th colspan="3">SA-6: Software Usage Restrictions</th></tr>
<tr><td colspan="3"><b>Control</b></td></tr>
<tr><td colspan="3">The organization:
a. Uses software and associated documentation in accordance with contract agreements and copyright laws;
b. Employs tracking systems for 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.</td></tr>
<tr><td colspan="3"><b>Guidance</b></td></tr>
<tr><td colspan="3">Tracking systems can include, for example, simple spreadsheets or fully automated, specialized applications depending on the needs of the organization.</td></tr>
<tr><td><b>Applicability:</b> Exchanges</td><td><b>Reference(s):</b> IRS-1075: 9.15</td><td><b>Related Control Requirements:</b></td></tr>
</table>

SA-6: Software Usage Restrictions
Assessment Procedure: SA-6.1
Assessment Objective
Determine if:
(i) the organization uses software and associated documentation in accordance with contract agreements and copyright laws; (ii) the organization employs tracking systems for software and associated documentation protected by quantity licenses to control copying and distribution; (iii) the organization 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.
Assessment Methods and Objects
Examine: System and services acquisition policy; procedures addressing software usage restrictions; site license documentation; list of software usage restrictions; other relevant documents or records.
Interview: Organizational personnel with information system administration responsibilities; organizational personnel operating, using, and/or maintaining the information system.

Table 201. SA-7: User-Installed Software

SA-7: User-Installed Software		
Control		
The organization prohibits users from downloading or installing software, unless explicitly authorized, in writing, by the CIO or his/her designated representative. If authorized, explicit rules govern the installation of software by users.		
Implementation Standards		
1. If user installed software is authorized, ensure that business rules and technical controls enforce the documented authorizations and prohibitions		
Guidance		
If provided the necessary privileges, users have the ability to install software. The organization identifies what types of software installations are permitted (e.g., updates and security patches to existing software) and what types of installations are prohibited (e.g., software whose pedigree with regard to being potentially malicious is unknown or suspect).		
Applicability: Exchanges	**Reference(s):**	**Related Control Requirements:** CM-2
Assessment Procedure: SA-7.1		
Assessment Objective		
Determine if:		
(i) the organization identifies and documents (as appropriate) explicit rules to be enforced when governing the installation of software by users; (ii) the organization (or information system) enforces explicit rules governing the installation of software by users. (iii) the organization meets all the requirements specified in the applicable implementation standard(s).		
Assessment Methods and Objects		
Examine: System and services acquisition policy; procedures addressing user installed software; list of rules governing user installed software; network traffic on the information system; other relevant documents or records.		
Interview: Organizational personnel with information system administration responsibilities; organizational personnel operating, using, and/or maintaining the information system.		

Table 202. SA-8: Security Engineering Principles

<table>
<tr><th colspan="3">SA-8: Security Engineering Principles</th></tr>
<tr><td colspan="3"><b>Control</b></td></tr>
<tr><td colspan="3">The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.</td></tr>
<tr><td colspan="3"><b>Guidance</b></td></tr>
<tr><td colspan="3">The application of security engineering principles is primarily targeted at new development information systems or systems undergoing major upgrades and is integrated into the system development life cycle. For legacy information systems, the organization applies security engineering principles to system upgrades and modifications to the extent feasible, given the current state of the hardware, software, and firmware within the system. Examples of 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 into the system development life cycle; (iv) delineating physical and logical security boundaries; (v) ensuring system developers and integrators are trained on how to develop secure software; (vi) tailoring security controls to meet organizational and operational needs; and (vii) reducing risk to acceptable levels, thus enabling informed risk management decisions.</td></tr>
<tr><td><b>Applicability:</b> Exchanges</td><td><b>Reference(s):</b> IRS-1075: 9.15</td><td><b>Related Control Requirements:</b></td></tr>
<tr><td colspan="3"><b>Assessment Procedure: SA-8.1</b></td></tr>
<tr><td colspan="3"><b>Assessment Objective</b></td></tr>
<tr><td colspan="3">Determine if:</td></tr>
<tr><td colspan="3">(i) the organization applies information system security engineering principles in the specification of the information system;
(ii) the organization applies information system security engineering principles in the design of the information system;
(iii) the organization applies information system security engineering principles in the development of the information system;
(iv) the organization applies information system security engineering principles in the implementation of the information system;
(v) the organization applies information system security engineering principles in the modification of the information system.</td></tr>
<tr><td colspan="3"><b>Assessment Methods and Objects</b></td></tr>
<tr><td colspan="3"><b>Examine:</b> System and services acquisition policy; procedures addressing security engineering principles used in the development and implementation of the information system; information system design documentation; security requirements and security specifications for the information system; other relevant documents or records.</td></tr>
<tr><td colspan="3"><b>Interview:</b> Organizational personnel with information system design, development, implementation, and modification responsibilities.</td></tr>
</table>

Table 203. SA-9: External Information System Services

SA-9: External Information System Services
Control
The organization prohibits service providers from outsourcing any system function outside the U.S. or its territories. If authorized the organization: a. Requires that providers of external information system services comply with organizational information security requirements and employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Defines and documents oversight and user roles and responsibilities with regard to external information system services; c. Ensures that service level agreements define expectations of performance, describe measurable outcomes, and identify remedies and response requirements for any identified instance of non-compliance; and d. Monitors security control compliance by external service providers. For FTI: FTI may not be accessed by agency employees, agents, representatives or contractors located “off-shore”,

SA-9: External Information System Services

outside of the United States or its territories. FTI may not be received, stored, processed or disposed via information technology systems located off-shore.

Implementation Standards

1. (For PHI only) A covered entity under HIPAA may permit a business associate to create, receive, maintain, or transmit EPHI on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with HIPAA regulations. Such assurances must be documented and meet the requirements set forth in HIPAA regulations. [See HIPAA 164.308(b) and 164.314(a).]

Guidance

An external information system service is a service that is implemented outside of the authorization boundary of the organizational information system (i.e., a service that is used by, but not a part of, the organizational information system). Relationships with external service providers are established in a variety of ways, for example, through joint ventures, business partnerships, outsourcing arrangements (i.e., contracts, interagency agreements, lines of business arrangements), licensing agreements, and/or supply chain exchanges. The responsibility for adequately mitigating risks arising from the use of external information system services remains with the authorizing official. Authorizing officials require that an appropriate chain of trust be established with external service providers when dealing with the many issues associated with information security. For services external to the organization, a chain of trust requires that the organization 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 to the organization. The extent and nature of this chain of trust varies based on the relationship between the organization and the external provider. Where a sufficient level of trust cannot be established in the external services and/or service providers, the organization employs compensating security controls. The external information system services documentation includes government, service provider, and end user security roles and responsibilities, and any service-level agreements. Service level agreements define the expectations of performance for each required security control, describe measurable outcomes, and identify remedies and response requirements for any identified instance of noncompliance.

Applicability: Exchanges	**Reference(s):** HIPAA: 164.314(b)(2)(iii); IRS-1075: 9.15	**Related Control Requirements:** CA-3

Assessment Procedure: SA-9.1

Assessment Objective

Determine if:

(i) the organization prohibits service providers from outsourcing any system function outside the U.S. or its territories;

(ii) if authorized, the organization requires that providers of external information system services comply with organizational information security requirements and employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;

(iii) if authorized, the organization defines and documents government oversight, and user roles and responsibilities with regard to external information system services;

(iv) if authorized, the organization ensures that service level agreements define expectations of performance, describe measurable outcomes, and identify remedies and response requirements for any identified instance of non-compliance;

(v) if authorized, the organization monitors security control compliance by external service providers.

(vi) the organization meets all the requirements specified in the applicable implementation standard(s).

Assessment Methods and Objects

Examine: System and services acquisition policy; procedures addressing external information system services; acquisition contracts and service level agreements; organizational security requirements and security specifications for external provider services; security control assessment evidence from external providers of information system services; other relevant documents or records.

Examine: Business associate assurance documentation. [See HIPAA 164.308(b) and 164.314(a).]

Interview: Organizational personnel with system and services acquisition responsibilities; external providers of information system services.

Interview: Organizational personnel responsible for maintaining business associate assurance documentation. [See HIPAA 164.308(b) and 164.314(a).]

Table 204. SA-10: Developer Configuration Management

SA-10: Developer Configuration Management		
Control		
The organization requires that information system developers/integrators: a. Perform configuration management during information system design, development, implementation, and operation; b. Manage and control changes to the information system; c. Implement only organization-approved changes; d. Document approved changes to the information system; and e. Track security flaws and flaw resolution.		
Guidance		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.15	**Related Control Requirements:** CM-3, CM-4, CM-9
Assessment Procedure: SA-10.1		
Assessment Objective		
Determine if the organization requires that information system developers/integrators:		

(i) perform configuration management during information system:
– design;
– development;
– implementation; and
– operation;
(ii) manage and control changes to the information system during:
– design;
– development;
– implementation; and
– modification;
(iii) implement only organization-approved changes;
(iv) document approved changes to the information system; and
(v) track security flaws and flaw resolution.		

Assessment Methods and Objects		
Examine: System and services acquisition policy; procedures addressing information system developer/integrator configuration management; acquisition contracts and service level agreements; information system developer/integrator configuration management plan; security flaw tracking records; system change authorization records; other relevant documents or records.		
Interview: Organization personnel with information system security, acquisition, and contracting responsibilities; organization personnel with configuration management responsibilities.		

Table 205. SA-11: Developer Security Testing

<table>
<tr><th colspan="3">SA-11: Developer Security Testing</th></tr>
<tr><td colspan="3"><b>Control</b></td></tr>
<tr><td colspan="3">The organization requires that information system developers/integrators, in consultation with associated security personnel (including security engineers):
a. Create and implement a security test and evaluation plan in accordance with, but not limited to the, current procedures;
b. Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security control assessment process; and
c. Document the results of the security control assessment and flaw remediation processes.
For FTI: The agency must submit a request to the IRS Office of Safeguards for authority to use live data for testing, providing a detailed explanation of the safeguards in place to protect the FTI over the Internet to a customer.</td></tr>
<tr><td colspan="3"><b>Implementation Standards</b></td></tr>
<tr><td colspan="3">1. If the security control assessment results are used in support of the security authorization process for the information system, ensure that no security relevant modifications of the information systems have been made subsequent to the assessment and after selective verification of the results.
2. Use hypothetical data when executing test scripts or in a test environment that is configured to comply with the security controls as if it is a production environment.</td></tr>
<tr><td colspan="3"><b>Guidance</b></td></tr>
<tr><td colspan="3">Developmental security test results are used to the greatest extent feasible after verification of the results and recognizing that these results are impacted whenever there have been security-relevant modifications to the information system subsequent to developer testing. Test results may be used in support of the security authorization process for the delivered information system.</td></tr>
<tr><td><b>Applicability:</b> Exchanges</td><td><b>Reference(s):</b> IRS-1075: 9.15, 9.18.8</td><td><b>Related Control Requirements:</b> CA-2, SI-2</td></tr>
<tr><td colspan="3"><b>Assessment Procedure: SA-11.1</b></td></tr>
<tr><td colspan="3"><b>Assessment Objective</b></td></tr>
<tr><td colspan="3">Determine if the organization requires that information system developers/integrators, in consultation with associated security personnel (including security engineers):
(i) create and implement a security test and evaluation plan;
(ii) implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and
(iii) document the results of the security testing/evaluation and flaw remediation processes.</td></tr>
<tr><td colspan="3"><b>Assessment Methods and Objects</b></td></tr>
<tr><td colspan="3"><b>Examine:</b> System and services acquisition policy; procedures addressing information system developer/integrator security testing; acquisition contracts and service level agreements; information system developer/integrator security test plans; records of developer/integrator security testing results for the information system; security flaw tracking records; other relevant documents or records.</td></tr>
<tr><td colspan="3"><b>Interview:</b> Organizational personnel with developer security testing responsibilities.</td></tr>
</table>

System and Communications Protection (SC) – Technical

Table 206. SC-1: System and Communications Protection Policy and Procedures

SC-1: System and Communications Protection Policy and Procedures		
Control		
The organization develops, disseminates, and reviews/updates within every three-hundred-sixty-five (365) days: a. A formal, documented system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.		
Guidance		
This control is intended to produce the policy and procedures that are required for the effective implementation of security controls and control enhancements in the system and communications protection family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The system and communications protection policy can be included as part of the general information security policy for the organization. System and communications protection procedures can be developed for the security program in general and for a particular information system, when required. he organizational risk management strategy is a key factor in the development of the system and communications protection policy.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.16	**Related Control Requirements:**
Assessment Procedure: SC-1.1		
Assessment Objective		
Determine if:		
(i) the organization develops and formally documents system and communications protection policy; (ii) the organization system and communications protection policy addresses: – purpose; – scope; – roles and responsibilities; – management commitment; – coordination among organizational entities; – compliance; (iii) the organization disseminates formal documented system and communications protection policy to elements within the organization having associated system and communications protection roles and responsibilities; (iv) the organization develops and formally documents system and communications protection procedures; (v) the organization system and communications protection procedures facilitate implementation of the system and communications protection policy and associated system and communications protection controls; (vi) the organization disseminates formal documented system and communications protection procedures to elements within the organization having associated system and communications protection roles and responsibilities; (vii) the organization reviews/updates the system and communications protection policy and procedures within every three-hundred-sixty-five (365) days.		
Assessment Methods and Objects		
Examine: System and communications protection policy and procedures; other relevant documents or records.		
Interview: Organizational personnel with system and communications protection responsibilities.		

Table 207. SC-2: Application Partitioning

SC-2: Application Partitioning		
Control		
The information system separates user functionality (including user interface services [e.g., web services]) from information system management (e.g., database management systems) functionality.		
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 and is accomplished by using different computers, different central processing units, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate. An example of this type of separation is observed in web administrative interfaces that use separate authentication methods for users of any other information system resources. This may include isolating the administrative interface on a different domain and with additional access controls.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.16	**Related Control Requirements:**
Assessment Procedure: SC-2.1		
Assessment Objective		
Determine if the information system separates user functionality (including user interface services) from information system management functionality.		
Assessment Methods and Objects		
Examine: System and communications protection policy; procedures addressing application partitioning; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.		

Table 208. SC-4: Information in Shared Resources

SC-4: Information in Shared Resources
Control
The information system prevents unauthorized and unintended information transfer via shared system resources.
Implementation Standards
1. Ensure that users of shared system resources cannot intentionally or unintentionally access information remnants, including encrypted representations of information, produced by the actions of a prior user or system process acting on behalf of a prior user. Ensure that system resources shared between two (2) or more users are released back to the information system, and are protected from accidental or purposeful disclosure. For FTI: When authorized to make further disclosures is present (e.g., agents/contractors), information disclosed outside the organization must be recorded on a separate list that reflects to whom the disclosure was made, what was disclosed, and why and when it was disclosed. Organizations transmitting FTI from one computer to another need only identify the bulk records transmitted. This identification will contain the approximate number of personal records, the date of the transmissions, the best possible description of the records, and the name of the individual making/receiving the transmission.
Guidance
The purpose of this control is to prevent information, including encrypted representations of information, produced by the actions of a prior user/role (or the actions of a process acting on behalf of a prior user/role) from being available to any current user/role (or current process) that obtains access to a shared system resource (e.g., registers, main memory, secondary storage) after that resource has been released back to the information system. Control of information in shared resources is also referred to as object reuse. This control does not address: (i) information remanence, which refers to residual representation of data that has been in some way nominally erased or removed; (ii) covert channels where shared resources are manipulated to achieve a violation of information flow restrictions; or (iii) components in the information system for which there is only a single user/role.

SC-4: Information in Shared Resources		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.16	**Related Control Requirements:**
Assessment Procedure: SC-4.1		
Assessment Objective		
Determine if the information system prevents unauthorized and unintended information transfer via shared system resources.		
Assessment Methods and Objects		
Examine: System and communications protection policy; procedures addressing information remnance; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.		

Table 209. SC-5: Denial of Service Protection

SC-5: Denial of Service Protection		
Control		
The information system protects against or limits the effects of the following types of denial of service attacks defined on the following sites or in the following documents: a. SANS Organization www.sans.org/dosstep; b. SANS Organization's Roadmap to Defeating DDoS www.sans.org/dosstep/roadmap.php; and c. NIST CVE List http://checklists.nist.gov/home.cfm.		
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 devices on an organization's internal network from being directly affected by denial of service attacks. Employing increased capacity and bandwidth combined with service redundancy may reduce the susceptibility to some denial of service attacks.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.16	**Related Control Requirements:** SC-7
Assessment Procedure: SC-5.1		
Assessment Objective		
Determine if:		
(i) the organization defines the types of denial of service attacks (or provides references to sources of current denial of service attacks) that can be addressed by the information system; and (ii) the information system protects against or limits the effects of the organization-defined or referenced types of denial of service attacks.		
Assessment Methods and Objects		
Examine: System and communications protection policy; procedures addressing denial of service protection; information system design documentation; security plan; information system configuration settings and associated documentation; other relevant documents or records.		

Table 210. SC-7: Boundary Protection

SC-7: Boundary Protection

Control

The information system:

a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; and

b. Connects to external networks or information systems only through managed interfaces consisting of automated boundary protection devices arranged in accordance with an organizational security architecture.

Implementation Standards

1. Ensure that access to all proxies is denied, except for those hosts, ports, and services that are explicitly required.
2. Utilize stateful inspection/application firewall hardware and software.
3. Utilize firewalls from at least two (2) different vendors at the various levels within the network to reduce the possibility of compromising the entire network.

Guidance

Restricting external web traffic only to organizational web servers within managed interfaces and prohibiting external traffic that appears to be spoofing an internal address as the source are examples of restricting and prohibiting communications. Managed interfaces employing boundary protection devices include, for example, proxies, gateways, routers, firewalls, guards, or encrypted tunnels arranged in an effective security architecture (e.g., routers protecting firewalls and application gateways residing on a protected subnetwork commonly referred to as a demilitarized zone or DMZ).

The organization considers the intrinsically 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 include third-party provided access lines and other service elements. Consequently, such interconnecting transmission services may represent sources of increased risk despite contract security provisions. When this situation occurs, the organization implements appropriate compensating security controls.

Applicability: Exchanges	**Reference(s):** IRS-1075: 9.16	**Related Control Requirements:** AC-4, CA-3, MP-4, RA-2

Assessment Procedure: SC-7.1

Assessment Objective

Determine if:

(i) the organization defines the external boundary of the information system;

(ii) the organization defines key internal boundaries of the information system;

(iii) the information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system;

(iv) the information system connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

(v) the organization meets all the requirements specified in the applicable implementation standard(s).

Assessment Methods and Objects

Examine: System and communications protection policy; procedures addressing boundary protection; list of key internal boundaries of the information system; information system design documentation; boundary protection hardware and software; information system configuration settings and associated documentation; enterprise security architecture documentation; other relevant documents or records.

Interview: Selected organizational personnel with boundary protection responsibilities.

Table 211. SC-7(1): Subnetworks for Publicly-Accessible Components

SC-7(1): Subnetworks for Publicly-Accessible Components		
Control		
The organization physically allocates publicly accessible Exchange information system components to separate subnetworks with separate physical network interfaces.		
Guidance		
Publicly accessible information system components include, for example, public web servers.		
Applicability: Exchanges	**Reference(s):**	**Related Control Requirements:**
Assessment Procedure: SC-7(1).1		
Assessment Objective		
Determine if the organization physically allocates publicly accessible information system components to separate subnetworks with separate, physical network interfaces.		
Assessment Methods and Objects		
Examine: System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system hardware and software; information system architecture; information system configuration settings and associated documentation; other relevant documents or records.		

Table 212. SC-7(2): Public Access into the Internal Networks

SC-7(2): Public Access into the Internal Networks		
Control		
The information system prevents public access into the organization's internal networks except as appropriately mediated by managed interfaces employing boundary protection devices.		
Applicability: Exchanges	**Reference(s):**	**Related Control Requirements:**
Assessment Procedure: SC-7(2).1		
Assessment Objective		
Determine if:		
(i) the organization defines the mediation necessary for public access to the organization's internal networks; (ii) the information system prevents public access into the organization's internal networks except as appropriately mediated by managed interfaces employing boundary protection devices.		
Assessment Methods and Objects		
Examine: System and communications protection policy; procedures addressing boundary protection; list of mediation vehicles for allowing public access to the organization's internal networks; information system design documentation; boundary protection hardware and software; information system configuration settings and associated documentation; other relevant documents or records.		

Table 213. SC-7(3): Limit System Access Points

<table>
<tr><th colspan="3">SC-7(3): Limit System Access Points</th></tr>
<tr><td colspan="3"><b>Control</b></td></tr>
<tr><td colspan="3">The organization limits the number of access points to the information system (e.g., prohibiting desktop modems) to allow for more comprehensive monitoring of inbound and outbound communications and network traffic.</td></tr>
<tr><td colspan="3"><b>Guidance</b></td></tr>
<tr><td colspan="3">The Trusted Internet Connection (TIC) initiative is an example of limiting the number of managed network access points.</td></tr>
<tr><td><b>Applicability:</b> Exchanges</td><td><b>Reference(s):</b></td><td><b>Related Control Requirements:</b></td></tr>
<tr><td colspan="3"><b>Assessment Procedure: SC-7(3).1</b></td></tr>
<tr><td colspan="3"><b>Assessment Objective</b></td></tr>
<tr><td colspan="3">Determine if the organization limits the number of access points to the information system to allow for more comprehensive monitoring of inbound and outbound communications and network traffic.</td></tr>
<tr><td colspan="3"><b>Assessment Methods and Objects</b></td></tr>
<tr><td colspan="3"><b>Examine:</b> System and communications protection policy; procedures addressing boundary protection; information system design documentation; boundary protection hardware and software; information system architecture and configuration documentation; information system configuration settings and associated documentation; communications and network traffic monitoring logs; other relevant documents or records.</td></tr>
</table>

Table 214. SC-7(4): Managed External Telecom Service Interface

<table>
<tr><th colspan="3">SC-7(4): Managed External Telecom Service Interface</th></tr>
<tr><td colspan="3"><b>Control</b></td></tr>
<tr><td colspan="3">The organization:
a. Implements a managed interface for each external telecommunication service;
b. Establishes a traffic flow policy for each managed interface;
c. Employs security controls as needed to protect the confidentiality and integrity of the information being transmitted;
d. Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need;
e. Reviews exceptions to the traffic flow policy within every three-hundred-sixty-five (365) days; and
f. Removes traffic flow policy exceptions that are no longer supported by an explicit mission/business need.</td></tr>
<tr><td><b>Applicability:</b> Exchanges</td><td><b>Reference(s):</b></td><td><b>Related Control Requirements:</b></td></tr>
<tr><td colspan="3"><b>Assessment Procedure: SC-7(4).1</b></td></tr>
<tr><td colspan="3"><b>Assessment Objective</b></td></tr>
<tr><td colspan="3">Determine if:</td></tr>
<tr><td colspan="3">(i) the organization implements a managed interface for each external telecommunication service;
(ii) the organization establishes a traffic flow policy for each managed interface;
(iii) the organization employs security controls as needed to protect the confidentiality and integrity of the information being transmitted;
(iv) the organization documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need;
(v) the organization reviews exceptions to the traffic flow policy within every three-hundred-sixty-five (365) days;
(vi) the organization removes traffic flow policy exceptions that are no longer supported by an explicit mission/business need.</td></tr>
</table>

SC-7(4): Managed External Telecom Service Interface
Assessment Methods and Objects
Examine: System and communications protection policy; procedures addressing boundary protection; traffic flow policy; information system security architecture; information system design documentation; boundary protection hardware and software; information system architecture and configuration documentation; information system configuration settings and associated documentation; records of traffic flow policy exceptions; other relevant documents or records.
Interview: Selected organizational personnel with boundary protection responsibilities.

Table 215. SC-7(5): Managed Interfaces Network Traffic Control

SC-7(5): Managed Interfaces Network Traffic Control		
Control		
The information system at managed interfaces, denies network traffic by default and allows network traffic by exception (i.e., deny all, permit by exception).		
Applicability: Exchanges	**Reference(s):**	**Related Control Requirements:**
Assessment Procedure: SC-7(5).1		
Assessment Objective		
Determine if:		
(i) the information system, at managed interfaces, denies network traffic by default; (ii) the information system, at managed interfaces, allows network traffic by exception.		
Assessment Methods and Objects		
Examine: System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.		
Interview: Selected organizational personnel with boundary protection responsibilities.		

Table 216. SC-7(6): Boundary Protection

SC-7(6): Boundary Protection		
Control		
The organization prevents the unauthorized release of information outside of the information system boundary or any unauthorized communication through the information system boundary when there is an operational failure of the boundary protection mechanisms.		
Applicability: Exchanges	**Reference(s):**	**Related Control Requirements:**
Assessment Procedure: SC-7(6).1		
Assessment Objective		
Determine if:		
(i) the organization prevents the unauthorized release of information outside of the information system boundary; or (ii) the organization prevents any unauthorized communication through the information system boundary when there is an operational failure of the boundary protection mechanisms.		
Assessment Methods and Objects		
Examine: System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.		

Table 217. SC-7(7): Boundary Protection

SC-7(7): Boundary Protection		
Control		
The information system prevents remote devices that have established a non-remote connection with the system from communicating outside of that communications path with resources in external networks.		
Applicability: Exchanges	**Reference(s):**	**Related Control Requirements:**
Assessment Procedure: SC-7(7).1		
Assessment Objective		
Determine if the information system prevents remote devices that have established a non-remote connection with the system from communicating outside of that communications path with resources in external networks.		
Assessment Methods and Objects		
Examine: System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system hardware and software; information system architecture; information system configuration settings and associated documentation; other relevant documents or records.		

Table 218. SC-8: Transmission Integrity

SC-8: Transmission Integrity		
Control		
The information system protects the integrity of transmitted information.		
Implementation Standards		
1. Employ appropriate approved mechanisms (e.g., digital signatures, cryptographic hashes) to protect the integrity of data while in transit from source to destination outside of a secured network (see SC-13). 2. For FTI: All FTI in transit must be encrypted when moving across a Wide Area Network (WAN) and within the agency's Local Area Network (LAN). If encryption is not used, the agency must use other compensating mechanisms (e.g. switched VLAN technology, fiber optic medium, etc.) to ensure FTI is not accessible to unauthorized users. (Pub 1075, ref. 9.18.2) 3. For FTI: FTI should not be transmitted or used on the agency's internal e-mail systems. If transmittal of FTI within the agency's e-mail system is necessary, specific precautions must be taken to protect the FTI. FTI must not be transmitted outside of the agency, either in the body of an e-mail or as an attachment. (Pub. 1075, Ref 9.18.5) 4. For FTI: The agency must follow specific precautions when faxing FTI. (Pub 1075 section 9.18.6)		
Guidance		
This control applies to communications across internal and external networks. If the organization is relying on a commercial service provider for transmission services as a commodity item rather than a fully dedicated service, it may be more difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission integrity. When it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.16, 9.18.2, 9.18.5, 9.18.6	**Related Control Requirements:** AC-17, PE-4
Assessment Procedure: SC-8.1		
Assessment Objective		
Determine if the information system protects the integrity of transmitted information.		

SC-8: Transmission Integrity
Assessment Methods and Objects
Examine: System and communications protection policy; procedures addressing transmission integrity; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

Table 219. SC-8(1): Transmission Integrity

SC-8(1): Transmission Integrity		
Control		
The organization employs cryptographic mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures.		
Guidance		
Alternative physical protection measures include, for example, protected distribution systems.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.16	**Related Control Requirements:** SC-13
Assessment Procedure: SC-8(1).1		
Assessment Objective		
Determine if the organization employs cryptographic mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures.		
Assessment Methods and Objects		
Examine: System and communications protection policy; procedures addressing transmission integrity; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.		

Table 220. SC-9: Transmission Confidentiality

SC-9: Transmission Confidentiality
Control
The information system protects the confidentiality of transmitted information. For FTI: 1. All FTI in transit must be encrypted when moving across a Wide Area Network (WAN) and within the agency's Local Area Network (LAN). If encryption is not used, the agency must use other compensating mechanisms (e.g. switched VLAN technology, fiber optic medium, etc.) to ensure FTI is not accessible to unauthorized users. 2. FTI should not be transmitted or used on the agency's internal e-mail systems. If transmittal of FTI within the agency's e-mail system is necessary, specific precautions must be taken to protect the FTI. FTI must not be transmitted outside of the agency, either in the body of an e-mail or as an attachment. 3. The agency must follow specific precautions when faxing FTI.
Implementation Standards
1. (For PII only) When sending or receiving faxes containing PII: (i) fax machines must be located in a locked room with a trusted staff member having custodial coverage over outgoing and incoming transmissions or fax machines must be located in a secured area; (ii) accurate broadcast lists and other preset numbers of frequent fax recipients must be maintained; and (iii) a cover sheet must be used that explicitly provides guidance to the recipient that includes: a notification of the sensitivity of the data and the need for protection, and a notice to unintended recipients to telephone the sender (collect if necessary) to report the disclosure and confirm destruction of the information.

<table>
<tr><th colspan="3">SC-9: Transmission Confidentiality</th></tr>
<tr><td colspan="3"><b>Guidance</b></td></tr>
<tr><td colspan="3">This control applies to communications across internal and external networks. If the organization is relying on a commercial service provider for transmission services as a commodity item rather than a fully dedicated service, it may be more difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission confidentiality. When it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, the organization implements appropriate compensating security controls.</td></tr>
<tr><td><b>Applicability:</b> Exchanges</td><td><b>Reference(s):</b> HIPAA: 164.312(e)(1); IRS-1075: 9.18.2, 9.18.5, 9.18.6</td><td><b>Related Control Requirements:</b> AC-17</td></tr>
<tr><td colspan="3"><b>Assessment Procedure: SC-9.1</b></td></tr>
<tr><td colspan="3"><b>Assessment Objective</b></td></tr>
<tr><td colspan="3">Determine if:</td></tr>
<tr><td colspan="3">(i) the information system protects the confidentiality of transmitted information.
(ii) the organization meets all the requirements specified in the applicable implementation standard(s).</td></tr>
<tr><td colspan="3"><b>Assessment Methods and Objects</b></td></tr>
<tr><td colspan="3"><b>Examine:</b> System and communications protection policy; procedures addressing transmission confidentiality; information system design documentation; contracts for telecommunications services; information system configuration settings and associated documentation; other relevant documents or records.</td></tr>
<tr><td colspan="3"><b>Examine:</b> Fax machine locations for secure custodial coverage of outgoing and incoming PII transmitted data.</td></tr>
</table>

Table 221. SC-9(1): Encrypt Data During Transmission

<table>
<tr><th colspan="3">SC-9(1): Encrypt Data During Transmission</th></tr>
<tr><td colspan="3"><b>Control</b></td></tr>
<tr><td colspan="3">The organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures.</td></tr>
<tr><td><b>Applicability:</b> Exchanges</td><td><b>Reference(s):</b> HIPAA: 164.312(e)(1), 164.312(e)(2)(ii); IRS-1075: 9.16</td><td><b>Related Control Requirements:</b> SC-13</td></tr>
<tr><td colspan="3"><b>Assessment Procedure: SC-9(1).1</b></td></tr>
<tr><td colspan="3"><b>Assessment Objective</b></td></tr>
<tr><td colspan="3">Determine if:</td></tr>
<tr><td colspan="3">(i) the organization optionally defines alternative physical measures to prevent unauthorized disclosure of information during transmission;
(ii) the organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by organization-defined alternative physical measures.</td></tr>
<tr><td colspan="3"><b>Assessment Methods and Objects</b></td></tr>
<tr><td colspan="3"><b>Examine:</b> System and communications protection policy; procedures addressing transmission confidentiality; information system design documentation; information system communications hardware and software or Protected Distribution System protection mechanisms; information system configuration settings and associated documentation; other relevant documents or records.</td></tr>
</table>

Table 222. SC-10: Network Disconnect

SC-10: Network Disconnect		
Control		
The information system automatically terminates the network connection associated with a communications session at the end of the session, or: a. Forcibly de-allocates communications session Dynamic Host Configuration Protocol (DHCP) leases after seven (7) days; and b. Forcibly disconnects inactive Virtual Private Network (VPN) connections after thirty (30) minutes of inactivity. For FTI: Forcibly disconnects inactive VPN connections after 15 minutes of inactivity.		
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. The time period of inactivity may, as the organization deems necessary, be a set of time periods by type of network access or for specific accesses.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.16	**Related Control Requirements:**
Assessment Procedure: SC-10.1		
Assessment Objective		
Determine if:		
(i) the organization defines the time period of inactivity before the information system terminates a network connection associated with a communications session; and (ii) the information system terminates a network connection associated with a communication session at the end of the session or after the organization-defined time period of inactivity.		
Assessment Methods and Objects		
Examine: System and communications protection policy; procedures addressing network disconnect; information system design documentation; organization-defined time period of inactivity before network disconnect; information system configuration settings and associated documentation; other relevant documents or records.		

Table 223. SC-12: Cryptographic Key Establishment and Management

SC-12: Cryptographic Key Establishment and Management		
Control		
When cryptography is required and used within the information system, the organization establishes and manages cryptographic keys for required cryptography employed within the information system.		
Guidance		
Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures. In addition to being required for the effective operation of a cryptographic mechanism, effective cryptographic key management provides protections to maintain the availability of the information in the event of the loss of cryptographic keys by users.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.16	**Related Control Requirements:**
Assessment Procedure: SC-12.1		
Assessment Objective		
Determine if the organization establishes and manages cryptographic keys for required cryptography employed within the information system.		

SC-12: Cryptographic Key Establishment and Management
Assessment Methods and Objects
Examine: System and communications protection policy; procedures addressing cryptographic key management and establishment; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.
Interview: Organizational personnel with responsibilities for cryptographic key establishment or management.

Table 224. SC-13: Use of Cryptography

SC-13: Use of Cryptography		
Control		
When cryptographic mechanisms are used, the information system implements required cryptographic protections using cryptographic modules that comply with applicable federal standards, and guidance.		
Applicability: Exchanges	**Reference(s):** HIPAA: 164.312(a)(2)(iv), 164.312(e)(2)(ii); IRS-1075: 9.16	**Related Control Requirements:** AC-3, SC-9(1)
Assessment Procedure: SC-13.1		
Assessment Objective		
Determine if when cryptographic mechanisms are used, the information system implements cryptographic protections using cryptographic modules that comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.		
Assessment Methods and Objects		
Examine: System and communications protection policy; procedures addressing use of cryptography; information system design documentation; information system configuration settings and associated documentation; cryptographic module validation certificates; other relevant documents or records.		

Table 225. SC-13(1): Use of Cryptography

SC-13(1): Use of Cryptography		
Control		
When cryptographic mechanisms are used, the organization employs, at a minimum, FIPS 140-2 compliant and NIST-validated cryptography to protect unclassified information.		
Guidance		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.16	**Related Control Requirements:** SC-13
Assessment Procedure: SC-13(1).1		
Assessment Objective		
Determine if the organization employs, at a minimum, FIPS-validated cryptography to protect unclassified information.		
Assessment Methods and Objects		
Examine: System and communications protection policy; procedures addressing use of cryptography; FIPS cryptography standards; information system design documentation; information system configuration settings and associated documentation; cryptographic module validation certificates; other relevant documents or records.		

Table 226. SC-14: Public Access Protections

SC-14: Public Access Protections		
Control		
The information system protects the integrity and availability of publicly available information and applications		
Implementation Standards		
1. Ensure that network access controls, operating system file permissions, and application configurations protect the integrity of information stored, processed, and transmitted by publicly accessible systems, as well as the integrity of publicly accessible applications. 2. If e-authentication is required and implemented in conjunction with or related to public access protections, refer to ARS Appendix D: E-authentication Standard.		
Guidance		
The purpose of this control is to ensure that organizations explicitly address the protection needs for public information and applications with such protection likely being implemented as part of other security controls.		
Applicability: Exchanges	**Reference(s):**	**Related Control Requirements:**
Assessment Procedure: SC-14.1		
Assessment Objective		
Determine if the information system protects the integrity and availability of publicly available information and applications.		
Assessment Methods and Objects		
Examine: System and communications protection policy; procedures addressing public access protections; access control policy and procedures; boundary protection procedures; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.		

Table 227. SC-15: Collaborative Computing Devices

SC-15: Collaborative Computing Devices		
Control		
The organization prohibits running collaborative computing mechanisms, unless explicitly authorized, in writing, by the CIO or his/her designated representative. If authorized, the authorization shall specifically identify allowed mechanisms, allowed purpose, and the information system upon which the mechanisms can be used. The information system: a. Prohibits remote activation of collaborative computing devices; and b. Provides an explicit indication of use to users physically present at the devices.		
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.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.16	**Related Control Requirements:**
Assessment Procedure: SC-15.1		
Assessment Objective		
Determine if when cryptographic mechanisms are used, the information system implements cryptographic protections using cryptographic modules that comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.		

SC-15: Collaborative Computing Devices
Assessment Methods and Objects
Examine: System and communications protection policy; procedures addressing use of cryptography; information system design documentation; information system configuration settings and associated documentation; cryptographic module validation certificates; other relevant documents or records.

Table 228. SC-15(1): Collaborative Computing Devices

SC-15(1): Collaborative Computing Devices		
Control		
If collaborative computing is authorized, the information system provides physical disconnect of collaborative computing devices in a manner that supports ease of use.		
Guidance		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.16	**Related Control Requirements:**
Assessment Procedure: SC-15(1).1		
Assessment Objective		
Determine if the information system provides physical disconnect of collaborative-computing devices in a manner that supports ease of use.		
Assessment Methods and Objects		
Examine: System and communications protection policy; procedures addressing collaborative computing; access control policy and procedures; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.		

Table 229. SC-17: Public Key Infrastructure Certificate

SC-17: Public Key Infrastructure Certificate		
Control		
When cryptographic mechanisms are used, the information system implements required cryptographic protections using cryptographic modules that comply with applicable federal standards, and guidance.		
Guidance		
For user certificates, each organization attains certificates from an approved, shared service provider, as required by OMB policy. For federal agencies operating a legacy public key infrastructure cross-certified with the Federal Bridge Certification Authority at medium assurance or higher, this Certification Authority will suffice. This control focuses on certificates with a visibility external to the information system and does not include certificates related to internal system operations, for example, application-specific time services.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.16	**Related Control Requirements:**
Assessment Procedure: SC-17.1		
Assessment Objective		
Determine if:		
(i) the organization defines a certificate policy for issuing public key certificates; and (ii) the organization issues public key certificates under the organization-defined certificate policy or obtains public key certificates under a certificate policy from an approved service provider.		

SC-17: Public Key Infrastructure Certificate
Assessment Methods and Objects
Examine: System and communications protection policy; procedures addressing public key infrastructure certificates; public key certificate policy or policies; public key issuing process; other relevant documents or records.
Interview: Organizational personnel with public key infrastructure certificate issuing responsibilities.

Table 230. SC-18: Mobile Code

<table>
<tr><th colspan="3">SC-18: Mobile Code</th></tr>
<tr><td colspan="3"><b>Control</b></td></tr>
<tr><td colspan="3">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.</td></tr>
<tr><td colspan="3"><b>Guidance</b></td></tr>
<tr><td colspan="3">Decisions regarding the employment of mobile code within information systems are based on the potential for the code to cause damage to the system if used maliciously. Mobile code technologies include, for example, Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidance apply to both the selection and use of mobile code installed on system servers and mobile code downloaded and executed on individual workstations. Policy and procedures related to mobile code, address preventing the development, acquisition, or introduction of unacceptable mobile code within the information system.</td></tr>
<tr><td><b>Applicability:</b> Exchanges</td><td><b>Reference(s):</b> IRS-1075: 9.16</td><td><b>Related Control Requirements:</b></td></tr>
<tr><td colspan="3"><b>Assessment Procedure: SC-18.1</b></td></tr>
<tr><td colspan="3"><b>Assessment Objective</b></td></tr>
<tr><td colspan="3">Determine if:</td></tr>
<tr><td colspan="3">(i) the organization defines acceptable and unacceptable mobile code and mobile code technologies;
(ii) the organization establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies;
(iii) the organization authorizes, monitors, and controls the use of mobile code within the information system.</td></tr>
<tr><td colspan="3"><b>Assessment Methods and Objects</b></td></tr>
<tr><td colspan="3"><b>Examine:</b> System and communications protection policy; procedures addressing mobile code; mobile code usage restrictions, mobile code implementation policy and procedures; list of acceptable mobile code and mobile code technologies; other relevant documents or records.</td></tr>
<tr><td colspan="3"><b>Interview:</b> Organizational personnel with mobile code authorization, monitoring, and control responsibilities.</td></tr>
</table>

Table 231. SC-19: Voice Over Internet Protocol

SC-19: Voice Over Internet Protocol
Control
The organization prohibits the use of Voice over Internet Protocol (VoIP) technologies, unless explicitly authorized, in writing, by the CIO or his/her designated representative. If authorized, the organization: a. Establishes usage restrictions and implementation guidance for 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. For FTI: The agency must meet specific technical requirements to utilize a VoIP network that provides FTI to a customer (Pub 1075, Ref. 9.18.13)
Guidance

SC-19: Voice Over Internet Protocol		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.18.3	**Related Control Requirements:**
Assessment Procedure: SC-19.1		
Assessment Objective		
Determine if:		
(i) the organization 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 (ii) the organization authorizes, monitors, and controls the use of VoIP within the information system.		
Assessment Methods and Objects		
Examine: System and communications protection policy; procedures addressing VoIP; VoIP usage restrictions; other relevant documents or records.		
Interview: Organizational personnel with VoIP authorization and monitoring responsibilities.		

Table 232. SC-20: Secure Name / Address Resolution Service (Authoritative Source)

SC-20: Secure Name / Address Resolution Service (Authoritative Source)		
Control		
The information system provides additional data origin and integrity artifacts along with the authoritative data the system returns in response to name/address resolution queries.		
Guidance		
This control enables remote clients to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service. A domain name system (DNS) server is an example of an information system that provides name/address resolution service. Digital signatures and cryptographic keys are examples of additional artifacts. DNS resource records are examples of authoritative data. 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. The DNS security controls are consistent with, and referenced from, OMB M-08-23.		
Applicability: Exchanges	**Reference(s):**	**Related Control Requirements:**
Assessment Procedure: SC-20.1		
Assessment Objective		
Determine if the information system provides additional data origin and integrity artifacts along with the authoritative data the system returns in response to name/address resolution queries.		
Assessment Methods and Objects		
Examine: System and communications protection policy; procedures addressing secure name/address resolution service (authoritative source); information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.		

Table 233. SC-20(1): Secure Name/Address Resolution Service (Authoritative Source)

SC-20(1): Secure Name/Address Resolution Service (Authoritative Source)		
Control		
The information system provides additional data origin and integrity artifacts along with the authoritative data the system returns in response to name/address resolution queries		
Guidance		
This control enables remote clients to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service. A domain name system (DNS) server is an example of an information system that provides name/address resolution service. Digital signatures and cryptographic keys are examples of additional artifacts. DNS resource records are examples of authoritative data. 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. The DNS security controls are consistent with, and referenced from, OMB Memorandum 08-23.		
Applicability: Exchanges	**Reference(s):**	**Related Control Requirements:**
Assessment Procedure: SC-20(1).1		
Assessment Objective		
Determine if		
(i) the information system, when operating as part of a distributed, hierarchical namespace, provides the means to indicate the security status of child subspaces; and (ii) the information system, when operating as part of a distributed, hierarchical namespace, enable verification of a chain of trust among parent and child domains (if the child supports secure resolution services).		
Assessment Methods and Objects		
Examine: System and communications protection policy; procedures addressing secure name/address resolution service (authoritative source); information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.		

Table 234. SC-22: Architecture and Provisioning for Name/Address Resolution Service

SC-22: Architecture and Provisioning for Name/Address Resolution Service		
Control		
The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.		
Guidance		
A domain name system (DNS) server is an example of an information system that provides name/address resolution service. To eliminate single points of failure and to enhance redundancy, there are typically at least two authoritative domain name system (DNS) servers, one configured as primary and the other as secondary. Additionally, the two servers are commonly located in two different network subnets and geographically separated (i.e., not located in the same physical facility). With regard to role separation, DNS servers with an internal role, only process name/address resolution requests from within the organization (i.e., internal clients). DNS servers with an external role only process name/address resolution information requests from clients external to the organization (i.e., on the external networks including the Internet). The set of clients that can access an authoritative DNS server in a particular role is specified by the organization (e.g., by address ranges, explicit lists).		
Applicability: Exchanges	**Reference(s):**	**Related Control Requirements:**
Assessment Procedure: SC-22.1		
Assessment Objective		
Determine if:		

SC-22: Architecture and Provisioning for Name/Address Resolution Service
(i) the information systems that collectively provide name/address resolution service for an organization are fault tolerant; (ii) the information systems that collectively provide name/address resolution service for an organization implement internal/external role separation.
Assessment Methods and Objects
Examine: System and communications protection policy; procedures addressing architecture and provisioning for name/address resolution service; access control policy and procedures; information system design documentation; assessment results from independent, testing organizations; information system configuration settings and associated documentation; other relevant documents or records.

Table 235. SC-23: Session Authenticity

<table>
<tr><th colspan="3">SC-23: Session Authenticity</th></tr>
<tr><td colspan="3"><b>Control</b></td></tr>
<tr><td colspan="3">The information system provides mechanisms to protect the authenticity of communications sessions.</td></tr>
<tr><td colspan="3"><b>Guidance</b></td></tr>
<tr><td colspan="3">This control focuses on communications protection at the session, versus packet, level. The intent of this control is to establish grounds for confidence at each end of a communications session in the ongoing identity of the other party and in the validity of the information being transmitted. For example, this control addresses man-in-the-middle attacks including session hijacking or insertion of false information into a session. This control is only implemented where deemed necessary by the organization (e.g., sessions in service-oriented architectures providing web-based services).</td></tr>
<tr><td><b>Applicability:</b>
Exchanges</td><td><b>Reference(s):</b></td><td><b>Related Control Requirements:</b></td></tr>
<tr><td colspan="3"><b>Assessment Procedure: SC-23.1</b></td></tr>
<tr><td colspan="3"><b>Assessment Objective</b></td></tr>
<tr><td colspan="3">Determine if the information system provides mechanisms to protect the authenticity of communications sessions.</td></tr>
<tr><td colspan="3"><b>Assessment Methods and Objects</b></td></tr>
<tr><td colspan="3"><b>Examine:</b> System and communications protection policy; procedures addressing session authenticity; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.</td></tr>
</table>

Table 236. SC-28: Protection of Information at Rest

<table>
<tr><th colspan="3">SC-28: Protection of Information at Rest</th></tr>
<tr><td colspan="3"><b>Control</b></td></tr>
<tr><td colspan="3">The information system protects the confidentiality and integrity of information at rest.</td></tr>
<tr><td colspan="3"><b>Guidance</b></td></tr>
<tr><td colspan="3">This control is intended to address the confidentiality and integrity of information at rest in non-mobile devices and covers user information and system information. Information at rest refers to the state of information when it is located on a secondary storage device (e.g., disk drive, tape drive) within an information system. Configurations and/or rule sets for firewalls, gateways, intrusion detection/prevention systems, and filtering routers and authenticator content are examples of system information likely requiring protection. Organizations may choose to employ different mechanisms to achieve confidentiality and integrity protections, as appropriate.</td></tr>
<tr><td><b>Applicability:</b>
Exchanges</td><td><b>Reference(s):</b></td><td><b>Related Control Requirements:</b></td></tr>
<tr><td colspan="3"><b>Assessment Procedure: SC-28.1</b></td></tr>
<tr><td colspan="3"><b>Assessment Objective</b></td></tr>
<tr><td colspan="3">Determine if the information system protects the confidentiality and integrity of information at rest.</td></tr>
</table>

SC-28: Protection of Information at Rest
Assessment Methods and Objects
Examine: System and communications protection policy; procedures addressing protection of information at rest; information system design documentation; information system configuration settings and associated documentation; cryptographic mechanisms and associated configuration documentation; list of information at rest requiring confidentiality and integrity protections; other relevant documents or records.

Table 237. SC-32: Information System Partitioning

SC-32: Information System Partitioning		
Control		
The organization partitions the information system into components residing in separate physical domains (or environments) as deemed necessary.		
Guidance		
Information system partitioning is a part of a defense-in-depth protection strategy. An organizational assessment of risk guides the partitioning of information system components into separate physical domains (or environments). The security categorization also guides the selection of appropriate candidates for domain partitioning. Managed interfaces restrict or prohibit network access and information flow among partitioned information system components.		
Applicability: Exchanges	**Reference(s):**	**Related Control Requirements:** AC-4, SC-7
Assessment Procedure: SC-32.1		
Assessment Objective		
Determine if the organization partitions the information system into components residing in separate physical domains (or environments) as deemed necessary.		
Assessment Methods and Objects		
Examine: System and communications protection policy; information system design documentation; information system configuration settings and associated documentation; information system architecture; list of information system physical domains (or environments); information system facility diagrams; other relevant documents or records.		
Interview: Organizational personnel installing, configuring, and/or maintaining the information system.		

Table 238. SC-ACA-1: Electronic Mail (Moderate)

SC-ACA-1: Electronic Mail (Moderate))		
Control		
Controls shall be implemented to protect ACA sensitive information (such as FTI or Privacy Act Protected information) that is sent via email.		
Implementation Standards		
1. Prior to sending an email, place all ACA sensitive information in an encrypted attachment.		
Guidance		
A good place to obtain recommended security practices for handling sensitive information via e-mail is NIST SP 800-45 (as amended), *Guidelines on Electronic Mail Security*.		
Applicability: All	**Reference(s):**	**Related Control Requirements:**
Assessment Procedure: SC-ACA.1		
Assessment Objective		
Determine if:		
(i) the organization effectively implements protections for ACA sensitive information that is sent via e-mail;		

SC-ACA-1: Electronic Mail (Moderate))
(ii) the organization meets all the requirements specified in the applicable implementation standard(s).
Assessment Methods and Objects
Examine: Email policy and procedures; other relevant documents or records.

System and Information Integrity (SI) – Operational

Table 239. SI-1: System and Information Integrity Policy and Procedures

SI-1: System and Information Integrity Policy and Procedures		
Control		
The organization develops, disseminates, and reviews/updates within every three-hundred-sixty-five (365) days: a. A formal, documented system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.		
Guidance		
This control is intended to produce the policy and procedures that are required for the effective implementation of security controls and control enhancements in the system and information integrity family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The system and information integrity policy can be included as part of the general information security policy for the organization. System and information integrity procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the system and information integrity policy.		
Applicability: Exchanges	**Reference(s):** HIPAA: 164.312(c)(1); IRS-1075: 9.17	**Related Control Requirements:**
Assessment Procedure: SI-1.1		
Assessment Objective		
Determine if:		
(i) the organization develops and formally documents system and information integrity policy; (ii) the organization system and information integrity policy addresses: – purpose; – scope; – roles and responsibilities; – management commitment; – coordination among organizational entities; – compliance; (iii) the organization disseminates formal documented system and information integrity policy to elements within the organization having associated system and information integrity roles and responsibilities; (iv) the organization develops and formally documents system and information integrity procedures; (v) the organization system and information integrity procedures facilitate implementation of the system and information integrity policy and associated system and information integrity controls; (vi) the organization disseminates formal documented system and information integrity procedures to elements within the organization having associated system and information integrity roles and responsibilities. (vii) the organization reviews/updates the system and information integrity policy and procedures within every three-hundred-sixty-five (365) days.		
Assessment Methods and Objects		
Examine: System and information integrity policy and procedures; other relevant documents or records.		
Interview: Organizational personnel with system and information integrity responsibilities.		

Table 240. SI-2: Flaw Remediation

SI-2: Flaw Remediation
Control
The organization: a. Identifies, reports, and corrects information system flaws; b. Tests software updates related to flaw remediation for effectiveness and potential side effects on

SI-2: Flaw Remediation		
information systems before installation; and c. Incorporates flaw remediation into the organizational configuration management process.		
Implementation Standards		
1. Correct identified information system flaws on production equipment in a timeframe based on the National Vulnerability Database (NVD) Vulnerability Severity Rating of the flaw: flaws rated as High severity within seven (7) calendar days; Medium severity within fifteen (15) calendar days; and all others within thirty (30) calendar days. 2. Evaluate system security patches, service packs, and hot fixes in a test bed environment to determine the effectiveness and potential side effects of such changes, and 3. Manage the flaw remediation process centrally.		
Guidance		
The organization identifies information systems containing software affected by recently announced software flaws (and potential vulnerabilities resulting from those flaws) and reports this information to designated organizational officials with information security responsibilities (e.g., senior information security officers, information system security managers, information systems security officers). The organization (including any contractor to the organization) promptly installs security-relevant software updates (e.g., patches, service packs, and hot fixes). Flaws discovered during security assessments, continuous monitoring, incident response activities, or information system error handling, are also addressed expeditiously. Organizations are encouraged to use resources such as the Common Weakness Enumeration (CWE) or Common Vulnerabilities and Exposures (CVE) databases in remediating flaws discovered in organizational information systems. By requiring that flaw remediation be incorporated into the organizational configuration management process, it is the intent of this control that required/anticipated remediation actions are tracked and verified. An example of expected flaw remediation that would be so verified is whether the procedures contained in US- CERT guidance and Information Assurance Vulnerability Alerts have been accomplished.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.17	**Related Control Requirements:** CA-2, CA-7, CM-3, MA-2, IR-4, RA-5, SA-11, SI-11.
Assessment Procedure: SI-2.1		
Assessment Objective		
Determine if		
(i) the organization identifies, reports, and corrects information system flaws; (ii) the organization tests software updates related to flaw remediation for effectiveness before installation; (iii) the organization tests software updates related to flaw remediation for potential side effects on organizational information systems before installation; and (iv) the organization incorporates flaw remediation into the organizational configuration management process.		
Assessment Methods and Objects		
Examine: System and information integrity policy; procedures addressing flaw remediation; list of flaws and vulnerabilities potentially affecting the information system; list of recent security flaw remediation actions performed on the information system (e.g., list of installed patches, service packs, hot fixes, and other software updates to correct information system flaws); test results from the installation of software to correct information system flaws; other relevant documents or records		
Interview: Organizational personnel with flaw remediation responsibilities.		

Table 241. SI-2(1): Flaw Remediation

SI-2(1): Flaw Remediation
Control
The organization centrally manages the flaw remediation process and installs software updates automatically.
Guidance
Due to information system integrity and availability concerns, organizations give careful consideration to the

SI-2(1): Flaw Remediation		
methodology used to carry out automatic updates.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.17	**Related Control Requirements:**
Assessment Procedure: SI-2(1).1		
Assessment Objective		
Determine if		
(i) the organization centrally manages the flaw remediation process; and (ii) the organization installs software updates automatically.		
Assessment Methods and Objects		
Examine: System and information integrity policy; procedures addressing flaw remediation; automated mechanisms supporting centralized management of flaw remediation and automatic software updates; information system design documentation; information system configuration settings and associated documentation; list of information system flaws; list of recent security flaw remediation actions performed on the information system; other relevant documents or records.		

Table 242. SI-2(2): Flaw Remediation

SI-2(2): Flaw Remediation		
Control		
The organization employs automated mechanisms monthly to determine the state of information system components with regard to flaw remediation.		
Guidance		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.17	**Related Control Requirements:**
Assessment Procedure: SI-2(2).1		
Assessment Objective		
Determine if		
(i) the organization defines the frequency of employing automated mechanisms to determine the state of information system components with regard to flaw remediation; and (ii) the organization employs automated mechanisms in accordance with the organization-defined frequency to determine the state of information system components with regard to flaw remediation.		
Assessment Methods and Objects		
Examine: System and information integrity policy; procedures addressing flaw remediation; automated mechanisms supporting flaw remediation; information system design documentation; information system configuration settings and associated documentation; list of information system flaws; list of recent security flaw remediation actions performed on the information system; information system audit records; other relevant documents or records.		

Table 243. SI-3: Malicious Code Protection

SI-3: Malicious Code Protection
Control
The organization: a. Employs malicious code protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code: – Transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means; or – Inserted through the exploitation of information system vulnerabilities;

SI-3: Malicious Code Protection

b. Updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with configuration management policy and procedures;

c. Configures malicious code protection mechanisms to:
   - Perform critical system file scans during system boot, information system scans using the frequency specified in Implementation Standard 1, and real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with organizational security policy; and
   - Block and quarantine malicious code and send alert to administrator 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.

Implementation Standards

1. Desktop malicious code scanning software is configured to perform critical system file scans every twenty (24) hours.

Guidance

Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, and remote-access servers. Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats (e.g., UUENCODE, Unicode) or contained within a compressed file. Removable media includes, for example, USB devices, diskettes, or compact disks. A variety of technologies and methods exist to limit or eliminate the effects of malicious code attacks. Pervasive configuration management and strong 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 missions and business functions. Traditional malicious code protection mechanisms are not built to detect such code. In these situations, organizations must rely instead on other risk mitigation measures to include, for example, secure coding practices, trusted procurement processes, configuration management and control, and monitoring practices to help ensure that software does not perform functions other than those intended.

Applicability: Exchanges	**Reference(s):** IRS-1075: 9.17	**Related Control Requirements:**

Assessment Procedure: SI-3.1

Assessment Objective

Determine if:

(i) the organization employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code:
   - transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means; or
   - inserted through the exploitation of information system vulnerabilities;

(ii) the organization employs malicious code protection mechanisms at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code:
   - transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means; or
   - inserted through the exploitation of information system vulnerabilities;

SI-3: Malicious Code Protection
(iii) the organization updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with configuration management policy and procedures defined in CM-1; (iv) the organization defines one or more of the following actions to be taken in response to malicious code detection: – block malicious code; – quarantine malicious code; and/or – send alert to administrator; (v) the organization configures malicious code protection mechanisms to: – perform periodic scans of the information system in accordance with organization-defined frequency; – perform real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with organizational security policy; – take organization-defined action(s) in response to malicious code detection; (vi) the organization addresses the receipt of false positives during malicious code: – detection and eradication; – the resulting potential impact on the availability of the information system. (vii) the organization meets all the requirements specified in the applicable implementation standard(s).
Assessment Methods and Objects
Examine: System and information integrity policy; procedures addressing malicious code protection; malicious code protection mechanisms; records of malicious code protection updates; information system configuration settings and associated documentation; other relevant documents or records.
Interview: Organizational personnel with malicious code protection responsibilities.

Table 244. SI-3(1): Malicious Code Protection Management

SI-3(1): Malicious Code Protection Management		
Control		
The organization centrally manages malicious code protection mechanisms.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.17	**Related Control Requirements:**
Assessment Procedure: SI-3(1).1		
Assessment Objective		
Determine if the organization centrally manages malicious code protection mechanisms.		
Assessment Methods and Objects		
Examine: System and information integrity policy; procedures addressing malicious code protection; information system design documentation; malicious code protection mechanisms; records of malicious code protection updates; information system configuration settings and associated documentation; other relevant documents or records.		

Table 245. SI-3(2): Automated Updates for Malicious Code Protection

SI-3(2): Automated Updates for Malicious Code Protection		
Control		
The information system automatically updates malicious code protection mechanisms (including signature definitions).		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.17	**Related Control Requirements:**
Assessment Procedure: SI-3(2).1		
Assessment Objective		
Determine if the information system automatically updates malicious code protection mechanisms, including		

SI-3(2): Automated Updates for Malicious Code Protection
signature definitions.
Assessment Methods and Objects
Examine: System and information integrity policy; procedures addressing malicious code protection; information system design documentation; malicious code protection mechanisms; records of malicious code protection updates; information system configuration settings and associated documentation; other relevant documents or records.

Table 246. SI-3(3): Malicious Code Protection

SI-3(3): Malicious Code Protection		
Control		
The information system prevents non-privileged users from circumventing malicious code protection capabilities.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.17	**Related Control Requirements:**
Assessment Procedure: SI-3(3).1		
Assessment Objective		
Determine if the information system prevents non-privileged users from circumventing malicious code protection capabilities.		
Assessment Methods and Objects		
Examine: System and information integrity policy; procedures addressing malicious code protection; information system design documentation; malicious code protection mechanisms; records of malicious code protection updates; information system configuration settings and associated documentation; other relevant documents or records.		

Table 247. SI-4: Information System Monitoring

SI-4: Information System Monitoring
Control
The organization: a. Monitors events on the information system in accordance with Information Security Incident Handling and Breach Analysis/Notification Procedure and detects information system attacks; b. Identifies unauthorized use of the Exchange information system; c. Deploys monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization; d. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information; and e. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.
Implementation Standards
1. Install IDS devices at network perimeter points and host-based IDS sensors on critical servers.

SI-4: Information System Monitoring		
Guidance		
Information system monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at the system boundary (i.e., part of perimeter defense and boundary protection). Internal monitoring includes the observation of events occurring within the system (e.g., within internal organizational networks and system components). 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, audit record monitoring software, network monitoring software). Strategic locations for monitoring devices include, for example, at 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. The granularity of the information collected is determined by the organization based on its monitoring objectives and the capability of the information system to support such activities. An example of a specific type of transaction of interest to the organization with regard to monitoring is Hyper Text Transfer Protocol (HTTP) traffic that bypasses organizational HTTP proxies, when use of such proxies is required.		
Applicability: Exchanges	**Reference(s):** HIPAA: 164.308(a)(5)(ii)(B); IRS-1075: 9.17	**Related Control Requirements:** AC-4, AC-8, AC-17, AU-2, AU-6, SI-3, SI-7
Assessment Procedure: SI-4.1		
Assessment Objective		
Determine if:		
(i) the organization monitors events on the information system in accordance with Information Security Incident Handling and Breach Analysis/Notification Procedure and detects information system attacks; (ii) the organization identifies unauthorized use of the information system; (iii) the organization deploys monitoring devices: – strategically within the information system to collect organization-determined essential information; – at ad hoc locations within the system to track specific types of transactions of interest to the organization; (iv) the organization 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; (v) the organization obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal and state laws and regulations. (vi) the organization meets all the requirements specified in the applicable implementation standard(s).		
Assessment Methods and Objects		
Examine: System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; other relevant documents or records.		
Interview: Organizational personnel with information system monitoring responsibilities.		

Table 248. SI-4(1): Information System Monitoring

SI-4(1): Information System Monitoring		
Control		
The organization interconnects and configures individual intrusion detection tools into a system wide intrusion detection system using common protocols.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.17	**Related Control Requirements:**
Assessment Procedure: SI-4(1).1		
Assessment Objective		
Determine if the organization interconnects and configures individual intrusion detection tools into a system-wide intrusion detection system using common protocols.		
Assessment Methods and Objects		

SI-4(1): Information System Monitoring
Examine: System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; information system protocols; other relevant documents or records.

Table 249. SI-4(2): Information System Monitoring

SI-4(2): Information System Monitoring		
Control		
The organization employs automated tools to support near real-time analysis of events.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.17	**Related Control Requirements:**
Assessment Procedure: SI-4(2).1		
Assessment Objective		
Determine if the organization employs automated tools to support near real-time analysis of events.		
Assessment Methods and Objects		
Examine: System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; information system protocols documentation; other relevant documents or records.		

Table 250. SI-4(4): Inbound and Outbound Communications Monitoring

SI-4(4): Inbound and Outbound Communications Monitoring		
Control		
The information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions.		
Guidance		
Unusual/unauthorized activities or conditions include, for example, internal traffic that indicates the presence of malicious code within an information system or propagating among system components, the unauthorized export of information, or signaling to an external information system. Evidence of malicious code is used to identify potentially compromised information systems or information system components.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.17	**Related Control Requirements:**
Assessment Procedure: SI-4(4).1		
Assessment Objective		
Determine if:		
(i) the information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions. (ii) the information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions.		
Assessment Methods and Objects		
Examine: System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; information system protocols; other relevant documents or records.		

Table 251. SI-4(5): Real Time Alerts

SI-4(5): Real Time Alerts		
Control		
The Exchange information system provides near real-time alerts when the following indications of compromise or potential compromise occur: a. Presence of malicious code, b. Unauthorized export of information, c. Signaling to an external information system, or d. Potential intrusions.		
Guidance		
Alerts may be generated, depending on the organization-defined list of indicators, from a variety of sources, for example, audit records or input from malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers.		
Applicability: Exchanges	**Reference(s):**	**Related Control Requirements:**
Assessment Procedure: SI-4(5).1		
Assessment Objective		
Determine if:		
(i) the organization defines indicators of compromise or potential compromise to the security of the information system; (ii) the information system provides near real-time alerts when any of the organization-defined list of compromise or potential compromise indicators occurs.		
Assessment Methods and Objects		
Examine: System and information integrity policy; procedures addressing information system monitoring tools and techniques; security plan; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; other relevant documents or records.		

Table 252. SI-4(6): Information System Monitoring

SI-4(6): Information System Monitoring		
Control		
The information system prevents non-privileged users from circumventing intrusion detection and prevention capabilities.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.17	**Related Control Requirements:**
Assessment Procedure: SI-4(6).1		
Assessment Objective		
Determine if the information system prevents non-privileged users from circumventing intrusion detection and prevention capabilities.		
Assessment Methods and Objects		
Examine: System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; information system protocols; other relevant documents or records.		

Table 253. SI-5: Security Alerts, Advisories, and Directives

SI-5: Security Alerts, Advisories, and Directives		
Control		
The organization: a. Receives information system security alerts, advisories, and directives from designated 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 appropriate personnel; and d. Implements security directives in accordance with established time frames, or notifies the degree of noncompliance.		
Guidance		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.17	**Related Control Requirements:**
Assessment Procedure: SI-5.1		
Assessment Objective		
Determine if		
(i) the organization receives information system security alerts, advisories, and directives from designated external organizations on an ongoing basis; (ii) the organization generates internal security alerts, advisories, and directives; (iii) the organization defines personnel (identified by name and/or by role) who should receive security alerts, advisories, and directives; (iv) the organization disseminates security alerts, advisories, and directives to organization-identified personnel; and (v) the organization implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.		
Assessment Methods and Objects		
Examine: System and information integrity policy; procedures addressing security alerts and advisories; records of security alerts and advisories; other relevant documents or records.		
Interview: Organizational personnel with security alert and advisory responsibilities; organizational personnel implementing, operating, maintaining, administering, and using the information system.		

Table 254. SI-7: Software and Information Integrity

SI-7: Software and Information Integrity		
Control		
The information system detects unauthorized changes to software and information.		
Guidance		
The organization employs integrity verification applications on the information system to look for evidence of information tampering, errors, and omissions. The organization employs good software engineering practices with regard to commercial off-the-shelf integrity mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and uses tools to automatically monitor the integrity of the information system and the applications it hosts.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.17	**Related Control Requirements:**
Assessment Procedure: SI-7.1		
Assessment Objective		
Determine if the information system detects unauthorized changes to software and information.		
Assessment Methods and Objects		

SI-7: Software and Information Integrity
Examine: System and information integrity policy; procedures addressing software and information integrity; information system design documentation; information system configuration settings and associated documentation; integrity verification tools and applications documentation; other relevant documents or records.

Table 255. SI-7(1): Software and Information Integrity

SI-7(1): Software and Information Integrity		
Control		
The organization reassesses the integrity of software and information by performing daily integrity scans of the information system.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.17	**Related Control Requirements:**
Assessment Procedure: SI-7(1).1		
Assessment Objective		
Determine if:		
(i) the organization defines the frequency of integrity scans to be performed on the information system; and (ii) the organization reassesses the integrity of software and information by performing integrity scans of the information system in accordance with the organization-defined frequency.		
Assessment Methods and Objects		
Examine: System and information integrity policy; procedures addressing software and information integrity; security plan; information system configuration settings and associated documentation; integrity verification tools and applications documentation; records of integrity scans; other relevant documents or records.		

Table 256. SI-8: Spam Protection

SI-8: Spam Protection		
Control		
The organization: a. Employs spam protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, web accesses, or other common means; and b. Updates spam protection mechanisms (including signature definitions) when new releases are available in accordance with configuration management policy and procedures.		
Guidance		
Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, and remote-access servers.		
Applicability: Exchanges	**Reference(s):**	**Related Control Requirements:** SC-5, SI-3
Assessment Procedure: SI-8.1		
Assessment Objective		
Determine if		
(i) the organization employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, Web accesses, removable media, or other common means; (ii) the organization employs spam protection mechanisms at workstations, servers, or mobile computing devices on the network to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, Web accesses, removable media, or other common means; and (iii) the organization updates spam protection mechanisms (including signature definitions) when new releases are available in accordance with organizational configuration management policy and procedures defined in CM-1.		

SI-8: Spam Protection
Assessment Methods and Objects
Examine: System and information integrity policy; procedures addressing spam protection; information system design documentation; spam protection mechanisms; information system configuration settings and associated documentation; other relevant documents or records.
Interview: Organizational personnel with spam protection responsibilities.

Table 257. SI-8(1): Spam Protection

SI-8(1): Spam Protection		
Control		
The organization centrally manages spam protection mechanisms.		
Applicability: Exchanges	**Reference(s):**	**Related Control Requirements:**
Assessment Procedure: SI-8(1).1		
Assessment Objective		
Determine if the organization centrally manages spam protection mechanisms.		
Assessment Methods and Objects		
Examine: System and information integrity policy; procedures addressing spam protection; information system design documentation; spam protection mechanisms; information system configuration settings and associated documentation; other relevant documents or records.		

Table 258. SI-9: Information Input Restrictions

SI-9: Information Input Restrictions		
Control		
The organization restricts the capability to input information to the information system to authorized personnel.		
Guidance		
Restrictions on organizational personnel authorized to input information to the information system may extend beyond the typical access controls employed by the system and include limitations based on specific operational/project responsibilities.		
Applicability: Exchanges	**Reference(s):**	**Related Control Requirements:** AC-5, AC-6
Assessment Procedure: SI-9.1		
Assessment Objective		
Determine if the organization restricts the capability to input information to the information system to authorized personnel.		
Assessment Methods and Objects		
Examine: System and information integrity policy; procedures addressing information input restrictions; access control policy and procedures; separation of duties policy and procedures; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.		
Interview: Organizational personnel with responsibilities for implementing restrictions on individual authorizations to input information into the information system.		

Table 259. SI-10: Information Input Validation

SI-10: Information Input Validation		
Control		
The information system uses automated mechanisms to check the validity of information inputs for accuracy, completeness, validity, and authenticity as close to the point of origin as possible.		
Guidance		
Rules for checking the valid syntax and semantics of information system inputs (e.g., character set, length, numerical range, acceptable values) are in place to verify that inputs match specified definitions for format and content. Inputs passed to interpreters are prescreened to prevent the content from being unintentionally interpreted as commands.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.17	**Related Control Requirements:**
Assessment Procedure: SI-10.1		
Assessment Objective		
Determine if the information system uses automated mechanisms to check the validity of information inputs for accuracy, completeness, validity, and authenticity as close to the point of origin as possible.		
Assessment Methods and Objects		
Examine: System and information integrity policy; procedures addressing information validity; access control policy and procedures; separation of duties policy and procedures; documentation for automated tools and applications to verify validity of information; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.		

Table 260. SI-11: Error Handling

SI-11: Error Handling		
Control		
The information system: a. Identifies potentially security-relevant error conditions; b. Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries in error logs and administrative messages that could be exploited by adversaries; and c. Reveals error messages only to authorized personnel. For FTI: Generates error messages that provide information necessary for corrective actions in error logs and administrative messages.		
Guidance		
The structure and content of error messages are carefully considered by the organization. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements. Sensitive information includes, for example, account numbers, social security numbers, and credit card numbers.		
Applicability: Exchanges	**Reference(s):** IRS-1075: 9.17	**Related Control Requirements:**
Assessment Procedure: SI-11.1		
Assessment Objective		
Determine if:		
(i) the information system identifies potentially security-relevant error conditions; (ii) the organization defines sensitive or potentially harmful information that should not be contained in error logs and administrative messages; (iii) the information system generates error messages that provide information necessary for corrective actions without revealing organization-defined sensitive or potentially harmful information in error logs and administrative messages that could be exploited by adversaries; and (iv) the information system reveals error messages only to authorized personnel.		

SI-11: Error Handling
Assessment Methods and Objects
Examine: System and information integrity policy; procedures addressing information system error handling; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

Table 261. SI-12: Information Output Handling and Retention

SI-12: Information Output Handling and Retention		
Control		
The organization handles and retains both information within and output from the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.		
Implementation Standard		
1. Retain output, including, but not limited to audit records, system reports, business and financial reports, and business records, from the information system in accordance with Policy and all applicable National Archives and Records Administration (NARA) requirements.		
Guidance		
The output handling and retention requirements cover the full life cycle of the information, in some cases extending beyond the disposal of the information system. The National Archives and Records Administration provides guidance on records retention.		
Applicability: Exchanges	**Reference(s):**	**Related Control Requirements:** MP-2, MP-4
Assessment Procedure: SI-12.1		
Assessment Objective		
Determine if:		
(i) the organization handles both information within and output from the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements; and (ii) the organization retains both information within and output from the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.		
Assessment Methods and Objects		
Examine: System and information integrity policy; procedures addressing information system output handling and retention; media protection policy and procedures; information retention records, other relevant documents or records.		
Interview: Organizational personnel with information output handling and retention responsibilities.		

Program Management (PM) – Management

Table 262. PM-1: Information Security Program Plan

PM-1: Information Security Program Plan		
Control		
The organization: a. Develops and disseminates an organization-wide information security program plan that: – 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; – Provides sufficient information about the program management controls and common controls (including specification of parameters for any assignment and selection operations either explicitly or by reference) to enable an implementation that is unambiguously compliant with the intent of the plan and a determination of the risk to be incurred if the plan is implemented as intended; – Includes roles, responsibilities, management commitment, coordination among organizational entities, and compliance; – 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]; and c. Revises the plan to address organizational changes and problems identified during plan implementation or security control assessments.		
Guidance		
The information security program plan can be represented in a single document or compilation of documents at the discretion of the organization. The plan documents the organization-wide program management controls and organization-defined common controls. 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.		
Applicability: Exchanges	**Reference(s):**	**Related Control Requirements:** PM-8
Assessment Procedure: PM-1.1		
Assessment Objective		
Determine if:		
(i) the organization develops an information security program plan for the organization that: – provides an overview of the requirements for the security program; – provides a description of the security program management controls and common controls in place or planned for meeting security program requirements;		

PM-1: Information Security Program Plan
– provides sufficient information about the program management controls and common controls (including specification of parameters for any assignment and selection operations either explicitly or by reference) to enable an implementation that is unambiguously compliant with the intent of the plan and a determination of the risk to be incurred if the plan is implemented as intended; – includes roles, responsibilities, management commitment, coordination among organizational entities, and compliance; – 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; (ii) the organization defines the frequency of information security program plan reviews; (iii) the organization reviews the organization-wide information security program plan in accordance with the organization-defined frequency; (iv) the organization revises the plan to address organizational changes and problems identified during plan implementation or security control assessments; and (v) the organization disseminates the most recent information security program plan to appropriate entities in the organization.
Assessment Methods and Objects
Examine: Information security program policy; procedures addressing information security program plan development and implementation; procedures addressing information security program plan reviews and updates; information security program plan; program management controls documentation; common controls documentation; records of information security program plan reviews and updates; other relevant documents or Records.
Interview: Organizational personnel with security planning and plan implementation responsibilities for the information security program.

Table 263. PM-2: Senior Information Security Officer

<table>
<tr><th colspan="3">PM-2: Senior Information Security Officer</th></tr>
<tr><td colspan="3"><b>Control</b></td></tr>
<tr><td colspan="3">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.</td></tr>
<tr><td colspan="3"><b>Guidance</b></td></tr>
<tr><td colspan="3">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 organizational official as the Senior Information Security Officer or Chief Information Security Officer.</td></tr>
<tr><td><b>Applicability:</b>
Exchanges</td><td><b>Reference(s):</b></td><td><b>Related Control Requirements:</b></td></tr>
<tr><td colspan="3"><b>Assessment Procedure: PM-2.1: Senior Information Security Officer</b></td></tr>
<tr><td colspan="3"><b>Assessment Objective</b></td></tr>
<tr><td colspan="3">Determine if:</td></tr>
<tr><td colspan="3">(i) organization appoints a senior information security officer to coordinate, develop, implement, and maintain an organization-wide information security program; and
(ii) the organization empowers the senior information security officer with the mission and resources required to coordinate, develop, implement, and maintain an organization-wide information security program.</td></tr>
<tr><td colspan="3"><b>Assessment Methods and Objects</b></td></tr>
<tr><td colspan="3"><b>Examine:</b> Information security program policy; information security program plan; documentation addressing roles and responsibilities of the senior information security officer position; information security program mission statement; other relevant documents or records.</td></tr>
<tr><td colspan="3"><b>Interview:</b> Organizational person appointed to the senior information security officer position.</td></tr>
</table>

Table 264. PM-3: Information Security Resources

PM-3: Information Security Resources		
Control		
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.		
Guidance		
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.		
Applicability: Exchanges	**Reference(s):**	**Related Control Requirements:** PM-4, SA-2
Assessment Procedure: PM-3.1		
Assessment Objective		
Determine if:		
(i) the organization includes in its capital planning and investment requests the resources needed to implement the information security program; (ii) the organization documents all exceptions to the requirement that all capital planning and investment requests include the resources needed to implement the information security program; (iii) the organization employs a business case/Exhibit 300/Exhibit 53 to record the resources required; and (iv) the organization makes the required information security resources available for expenditure as planned.		
Assessment Methods and Objects		
Examine: Information security program policy; capital planning and investment policy; procedures addressing management and oversight for information security-related aspects of the capital planning and investment control process; capital planning and investment documentation; documentation of exceptions supporting capital planning and investment requests; business cases; Exhibit 300; Exhibit 53; other relevant documents or records].		
Interview: Organizational personnel managing and overseeing the information security related aspects of the capital planning and investment control process		

Table 265. PM-4: Plan of Action and Milestones Process

PM-4: Plan of Action and Milestones Process		
Control		
The organization implements a process for ensuring that plans of action and milestones for the security program and the associated organizational information systems are maintained and document the remedial information security actions to mitigate risk to organizational operations and assets, individuals, other organizations, and the Nation.		
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. The plan of action and milestones updates are based on the findings from security control assessments, security impact analyses, and continuous monitoring activities. OMB FISMA reporting guidance contains instructions regarding organizational plans of action and milestones.		
Applicability: Exchanges	**Reference(s):**	**Related Control Requirements:** CA-5
Assessment Procedure: PM-4.1		
Assessment Objective		
Determine if:		

PM-4: Plan of Action and Milestones Process
(i) the organization implements a process to maintain plans of action and milestones for the security program and the associated organizational information systems; and (ii) the organization implements a process to document the remedial information security actions that mitigate risk to organizational operations and assets, individuals, other organizations, and the Nation.
Assessment Methods and Objects
Examine: Information security program policy; plan of action and milestones policy; procedures addressing plan of action and milestones process; plan of action and milestones for the security program; plan of action and milestones for organizational information systems; other relevant documents or records.
Interview: Organizational personnel with plan of action and milestones development and implementation responsibilities.

Table 266. PM-5: Information System Inventory

PM-5: Information System Inventory		
Control		
The organization develops and maintains an inventory of its information systems.		
Guidance		
This control addresses the inventory requirements in FISMA. OMB provides guidance on developing information systems inventories and associated reporting requirements.		
Applicability: Exchanges	**Reference(s):**	**Related Control Requirements:**
Assessment Procedure: PM-5.1		
Assessment Objective		
Determine if:		
(i) the organization develops an inventory of its information systems; and (ii) the organization maintains an inventory of its information systems.		
Assessment Methods and Objects		
Examine: Information security program policy; procedures addressing information system inventory development and maintenance; information system inventory records, other relevant documents or records.		
Interview: Organizational personnel with information system inventory development and maintenance responsibilities.		

Table 267. PM-6: Information Security Measures of Performance

PM-6: Information Security Measures of Performance		
Control		
The organization develops, monitors, and reports on the results of information security measures of performance.		
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.		
Applicability: Exchanges	**Reference(s):**	**Related Control Requirements:**
Assessment Procedure: PM-6.1		
Assessment Objective		
Determine if:		
(i) the organization develops information security measures of performance; (ii) the organization monitors information security measures of performance; and (iii) the organization reports on the results of information security measures of performance.		

PM-6: Information Security Measures of Performance
Assessment Methods and Objects
Examine: Information security program policy; procedures addressing development, monitoring, and reporting of information security performance measures; information security performance metrics; information security performance measures; results of information security performance measures; other relevant documents or records.

Table 268. PM-7: Enterprise Architecture

PM-7: Enterprise Architecture		
Control		
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.		
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 also embeds into the enterprise architecture, a integral security architecture consistent with organizational risk management and information security strategies. Security requirements and 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.		
Applicability: Exchanges	**Reference(s):**	**Related Control Requirements:** PL-2, PM-11, RA-2
Assessment Procedure: PM-7.1		
Assessment Objective		
Determine if 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.		
Assessment Methods and Objects		
Examine: Information security program policy; enterprise architecture policy; procedures addressing information security-related aspects of enterprise architecture development; system development life cycle documentation; enterprise architecture documentation; enterprise security architecture documentation; other relevant documents or records.		

Table 269. PM-8: Critical Infrastructure Plan

PM-8: Critical Infrastructure Plan		
Control		
The organization addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.		
Guidance		
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.		
Applicability: Exchanges	**Reference(s):**	**Related Control Requirements:** PM-1, PM-9, PM-11, RA-3
Assessment Procedure: PM-8.1		
Assessment Objective		
Determine if:		

PM-8: Critical Infrastructure Plan
(i) the organization develops and documents a critical infrastructure and key resource protection plan; (ii) the organization updates the critical infrastructure and key resource protection plan; and (iii) the organization addresses information security issues in the critical infrastructure and key resource protection plan.
Assessment Methods and Objects
Examine: Information security program policy; critical infrastructure protection policy; procedures addressing critical infrastructure plan development and implementation; procedures addressing critical infrastructure plan reviews and updates; records of critical infrastructure plan reviews and updates; other relevant documents or records.
Interview: Organizational personnel with critical infrastructure plan development and implementation responsibilities.

Table 270. PM-9: Risk Management Strategy

<table>
<tr><th colspan="3">PM-9: Risk Management Strategy</th></tr>
<tr><td colspan="3"><b>Control</b></td></tr>
<tr><td colspan="3">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; and
b. Implements that strategy consistently across the organization.</td></tr>
<tr><td colspan="3"><b>Guidance</b></td></tr>
<tr><td colspan="3">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.</td></tr>
<tr><td><b>Applicability:</b> Exchanges</td><td><b>Reference(s):</b></td><td><b>Related Control Requirements:</b> RA-3</td></tr>
<tr><td colspan="3"><b>Assessment Procedure: PM-9.1</b></td></tr>
<tr><td colspan="3"><b>Assessment Objective</b></td></tr>
<tr><td colspan="3">Determine if:</td></tr>
<tr><td colspan="3">(i) the organization 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; and
(ii) the organization implements that strategy consistently across the organization.</td></tr>
<tr><td colspan="3"><b>Assessment Methods and Objects</b></td></tr>
<tr><td colspan="3"><b>Examine:</b> Information security program policy; risk management policy; procedures addressing risk management strategy development and implementation; risk management strategy (including risk identification, assessment, mitigation, acceptance, and monitoring methodologies); other relevant documents or records.</td></tr>
<tr><td colspan="3"><b>Interview:</b> Organizational personnel with risk management strategy development and implementation responsibilities.</td></tr>
</table>

Table 271. PM-10: Security Authorization Process

PM-10: Security Authorization Process		
Control		
The organization: a. Manages (i.e., documents, tracks, and reports) the security state of organizational information systems 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.		
Guidance		
The security authorization process for information systems requires the implementation of the Risk Management Framework and the employment of associated security standards and guidelines. Specific roles within the risk management process include a designated authorizing official for each organizational information system.		
Applicability: Exchanges	**Reference(s):**	**Related Control Requirements:** CA-6
Assessment Procedure: PM-10.1		
Assessment Objective		
Determine if:		
(i) the organization manages (i.e., documents, tracks, and reports) the security state of organizational information systems through security authorization processes; (ii) the organization designates individuals to fulfill specific roles and responsibilities within the organizational risk management process; and (iii) the organization fully integrates the security authorization processes into an organization-wide risk management program.		
Assessment Methods and Objects		
Examine: Information security program policy; security assessment and authorization policy; risk management policy; procedures addressing security authorization processes; security authorization package (including security plan, security assessment report, plan of action and milestones, authorization statement); other relevant documents or records.		
Interview: Organizational personnel with security authorization responsibilities for information systems; organizational personnel with risk management responsibilities.		

Table 272. PM-11: Mission/Business Process Definition

PM-11: Mission/Business Process Definition
Control
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 an achievable set of protection needs is obtained.
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.

<table>
<tr><th colspan="3">PM-11: Mission/Business Process Definition</th></tr>
<tr><td><b>Applicability:</b> Exchanges</td><td><b>Reference(s):</b></td><td><b>Related Control Requirements:</b> PM-7, PM-8, RA-2</td></tr>
<tr><td colspan="3"><b>Assessment Procedure: PM-11.1</b></td></tr>
<tr><td colspan="3"><b>Assessment Objective</b></td></tr>
<tr><td colspan="3">Determine if:</td></tr>
<tr><td colspan="3">(i) the organization 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
(ii) the organization determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.</td></tr>
<tr><td colspan="3"><b>Assessment Methods and Objects</b></td></tr>
<tr><td colspan="3"><b>Examine:</b> Information security program policy; risk management policy; procedures addressing security categorization of organizational information and information systems; organizational mission/business processes; risk management strategy (including risk identification, assessment, mitigation, acceptance, and monitoring methodologies); other relevant documents or records.</td></tr>
<tr><td colspan="3"><b>Interview:</b> Organizational personnel with mission/business process definition responsibilities; organizational personnel with security categorization and risk management responsibilities for the information security program.</td></tr>
</table>

Additional Controls Required by IRS Publication 1075

Table 273. Protection of FTI in Virtual Environment

Protection of FTI in Virtual Environment		
Control		
Notification Requirements a. The agency must notify the IRS Office of Safeguards 45 days prior to putting FTI in a virtual environment. b. If the agency's approved SPR is less than six years old and reflects the agency's current process, procedures and systems, the agency must submit the Virtualization Notification (see Exhibit 15), which will serve as an addendum to their SPR. c. If the agency's SPR is more than six years old or does not reflect the agency's current process, procedures and systems, the agency must submit a new SPR and the Virtualization Notification (see Exhibit 15). Technical Requirements a. When FTI is stored in a shared location, the agency must have policies in place to restrict access to FTI to authorized users. b. Programs that control the hypervisor should be secured and restricted to authorized administrators only. c. FTI data transmitted via hypervisor management communication systems on untrusted networks must be encrypted using FIPS-approved methods, provided by either the virtualization solution or third party-solution, such as a virtual private network (VPN) that encapsulates the management traffic. d. Separation between virtual machines (VMs) must be enforced, and functions which allow one VM to share data with the hypervisor or another VM, such as clipboard sharing or shared disks, must be disabled. e. Virtualization providers must be able to monitor for threats and other activity that is occurring within the virtual environment. This includes being able to monitor the movement of FTI into and out of the virtual environment. f. The VMs and hypervisor/ host OS software for each system within the virtual environment that receives, processes, stores or transmits FTI must be hardened in accordance with the requirements of Publication 1075 and be subject to frequent vulnerability testing. g. Special VM functions available to system administrators in a virtualized environment that can leverage the shared memory space in a virtual environment between the hypervisor and VM should be disabled. h. Virtual systems are configured to prevent FTI from being dumped outside of the VM when system errors occur. i. Vulnerability assessment must be performed on systems in a virtualized environment prior to system implementation. i. Backups (virtual machine snapshot) must be properly secured and must be stored in a logical location where the backup is only accessible to those with a need to know.		
Guidance		
Applicability: Exchanges	**Reference(s):** IRS-1075 9.18.12	**Related Control Requirements:**
Assessment Procedure:		
Assessment Objective		
Assessment objectives are documented in the Safeguards Computer Security Evaluation Matrix (SCSEM) for Virtual Environments.		
Assessment Methods and Objects		
Examine: Assessment methods and objects are documented in the Safeguards Computer Security Evaluation Matrix (SCSEM) for Virtual Environments.		
Interview: Assessment methods and objects are documented in the Safeguards Computer Security Evaluation Matrix (SCSEM) for Virtual Environments.		

Table 274. Protection of FTI in Voice Over IP (VOIP) Networks

Protection of FTI in Voice Over IP (VOIP) Networks		
Control		
a. VoIP traffic that contains FTI should be segmented off from non-VoIP traffic via a virtual Local Area Network (vLAN) or other segmentation method. If complete segmentation is not feasible, the agency must have compensating controls in place and properly applied which restrict access to VoIP traffic that contains FTI. b. When FTI is in-transit across the network (either Internet or state agency's network), the VoIP traffic must be encrypted using a NIST-approved method operating in a NIST-approved mode. c. VoIP network hardware (servers, routers, switches, firewalls) must be physically protected in accordance with the minimum protection standards for physical security outlined in IRS Publication 1075, section 4.0, Secure Storage. d. Each system within the agency's network that transmits FTI to an external customer through the VoIP network is hardened in accordance with the requirements of Publication 1075 and is subject to frequent vulnerability testing. e. VoIP-ready firewalls must be used to filter VoIP traffic on the network. f. Security testing must be conducted on the VoIP system prior to implementation with FTI and annually thereafter. g. VoIP phones must be logically protected and agencies must be able to track and audit all FTI-applicable conversations and access		
Guidance		
Applicability: Exchanges	**Reference(s):** IRS-1075 9.18.13	**Related Control Requirements:**
Assessment Procedure:		
Assessment Objective		
Assessment objectives are documented in the Safeguards Computer Security Evaluation Matrix (SCSEM) for VOIP Networks.		
Assessment Methods and Objects		
Examine: Assessment methods and objects are documented in the Safeguards Computer Security Evaluation Matrix (SCSEM) for VOIP Networks.		
Interview: Assessment methods and objects are documented in the Safeguards Computer Security Evaluation Matrix (SCSEM) for VOIP Networks.		

Table 275. Protection of FTI in Cloud Computing Environments

Protection of FTI in Cloud Computing Environments
Control
Notification Requirements a. The agency must notify the IRS Office of Safeguards 45 days prior to putting FTI in a cloud environment. b. If the agency's approved SPR is less than six years old and reflects the agency's current process, procedures and systems, the agency must submit the Cloud Computing Notification (see Exhibit 16), which will serve as an addendum to their SPR. c. If the agency's SPR is more than six years old or does not reflect the agency's current process, procedures and systems, the agency must submit a new SPR and the Cloud Computing Notification (see Exhibit 16). Technical Requirements d. Data Isolation. Software, data, and services that receive, transmit, process, or store FTI must be isolated within the cloud environment so that tenants sharing physical space cannot access their neighbors' physically co-located data and applications. e. Service Level Agreements (SLA). The agency must establish security policies and procedures based on IRS Publication 1075 for how FTI is stored, handled, and accessed inside the cloud through a legally

Protection of FTI in Cloud Computing Environments

binding contract or Service Level Agreement (SLA) with their third party cloud provider.

f. Data Encryption in Transit. FTI must be encrypted in transit within the cloud environment. All mechanisms used to encrypt FTI must be FIPS 140-2 compliant, and operate utilizing the FIPS 140-2 compliant module. This requirement must be included in the SLA.

g. Data Encryption at Rest. FTI must be encrypted while at rest in the cloud. All mechanisms used to encrypt FTI must be FIPS 140-2 compliant, and operate utilizing the FIPS 140-2 compliant module. This requirement must be included in the SLA.

h. Security Control Validation. Agencies must validate security control implementation claims made by cloud providers through a security plan and security control assessments.

Guidance

Applicability: Exchanges	**Reference(s):** IRS-1075 9.18.14	**Related Control Requirements:**

Assessment Procedure:

Assessment Objective

Assessment objectives are documented in the Safeguards Computer Security Evaluation Matrix (SCSEM) for cloud computing environments.

Assessment Methods and Objects

Examine: Assessment methods and objects are documented in the Safeguards Computer Security Evaluation Matrix (SCSEM) for cloud computing environments.

Interview: Assessment methods and objects are documented in the Safeguards Computer Security Evaluation Matrix (SCSEM) for cloud computing environments.