Centers for Medicare & Medicaid Services
Information Security and Privacy Group

Risk Management Handbook (RMH)
Chapter 14: Risk Assessment (RA)

Version 1.1

October 19, 2018

Record of Changes

The "Record of Changes" table below capture changes when updating the document. All columns are mandatory.

Version Number	Date	Chapter Section	Author/Owner Name	Description of Change
0.1	11/29/2017	All	ISPG	Initial Draft
0.2	01/03/2018	All	ISPG	Working Group Review
0.3	03/09/2018	Section 3.3	ISPG	Alignment with new HHS POAM Guidance
0.4	08/15/2018	All	ISPG	Update to new RMH template; inclusion of latest Risk Assessment-related audit findings and POA&Ms
1.0	10/01/2018	All	ISPG	Publication
1.1	10/19/2018	Section 6.2.3	ISPG	Update to guidance on SSP from NIST publication 800-18 to RMH Chapter 12 Security and Privacy Planning.

Effective Date/Approval

This Procedure becomes effective on the date that CMS's Deputy Chief Information Security Officer signs it and remains in effect until it is rescinded, modified or superseded.

Signature: /s/ Date of Issuance

Kevin Allen Dorsey
CMS Deputy Chief Information Security Officer
(DCISO)

Table of Contents

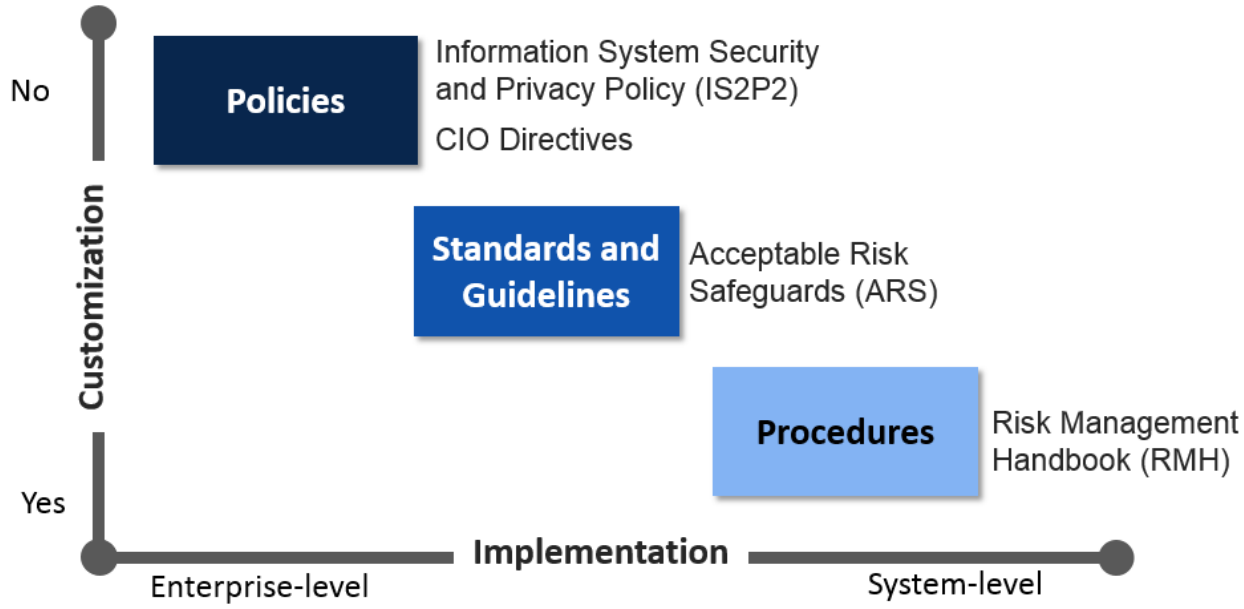
Tables

Figures

1. Introduction

1.1 Purpose

The Centers for Medicare & Medicaid Services (CMS) Risk Management Handbook (RMH) Chapter 14 Risk Assessment provides the procedures for implementing the requirements of the CMS Information Systems Security and Privacy Policy (IS2P2) and the CMS Acceptable Risk Safeguards (ARS). The following is a diagram that breaks down the hierarchy of the IS2P2, ARS, and RMH:



This document describes procedures that facilitate the implementation of security controls associated with the Risk Assessment (RA) family of controls. To promote consistency among all RMH Chapters, CMS intends for Chapter 14 to align with guidance from the National Institute of Standards and Technology (NIST). CMS incorporates the content of NIST's Special Publication (SP) 800-53, Security and Privacy Controls for Federal Information Systems and Organizations; and NIST SP 800-137 Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, into its governance documents, tailoring that content to the CMS environment.

1.2 Authority

The Federal Information Security Management Act (FISMA) requires each federal agency to develop, document and implement an agency-wide program to provide information security for the information and systems that support the operations and assets of the agency, including those provided or managed by another agency or contractor. The Federal Information Security Modernization Act of 2014 designates NIST with responsibility to develop guidance to federal agencies on information security and privacy requirements for federal information systems.

As an operating division of the Department of Health and Human Services (HHS), CMS must also comply with the HHS IS2P, Privacy Act of 1974 ("Privacy Act"), the Privacy and Security Rules developed pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and the E-Government Act of 2002, which relates specifically to electronic authentication requirements. The HHS Office for Civil Rights (OCR) is responsible for enforcement of the HIPAA Security and Privacy Rules. CMS seeks to comply with the requirements of these authorities, and to specify how CMS implements compliance in the CMS IS2P2.

HHS and CMS governance documents establish roles and responsibilities for addressing privacy and security requirements. In compliance with the HHS Information Systems Security and Privacy Policy (IS2P), the CMS Chief Information Officer (CIO) designates the CMS Chief Information Security Officer (CISO) as the CMS authority for implementing the CMS-wide information security program. HHS also designates the CMS Senior Official for Privacy (SOP) as the CMS authority for implementing the CMS-wide privacy program. Through their authority given by HHS, the CIO and SOP delegate authority and responsibility to specific organizations and officials within CMS to develop and administer defined aspects of the CMS Information Security and Privacy Program.

All CMS stakeholders must comply with and support the policies and the procedures referenced in this handbook to ensure compliance with federal requirements for implementation of information security and privacy controls.

1.3 Scope

This handbook documents procedures that facilitate the implementation of the privacy and security controls defined in the CMS IS2P2 and the CMS ARS. This RMH Chapter provides authoritative guidance on matters related to the Risk Assessment family of controls for use by CMS employees and contractors that support the development, operations, maintenance, and disposal of CMS information systems. This handbook does not supersede any applicable laws, existing labor management agreements, and/or higher-level agency directives or other governance documents.

1.4 Background

This handbook aligns with NIST SP 800-53 catalogue of controls, the CMS IS2P2, and the CMS ARS. Each procedure relates to a specific NIST security control family. Additional sections of this document crosswalk requirements to other control families and address specific audit requirements issued by various sources (e.g., OMB, OIG, HHS, etc.).

RMH Chapter 14 provides processes and procedures to assist with the consistent implementation of the RA family of controls for any system that stores, processes, or transmits CMS information on behalf of CMS. This chapter identifies the policies, minimum standards, and procedures for the effective implementation of selected security and privacy controls and control enhancements in the RA family.

CMS's comprehensive information security and privacy policy framework includes:

- An overarching policy (CMS IS2P2) that provides the foundation for the security and privacy principles and establishes the enforcement of rules that will govern the program and form the basis of the risk management framework
- Standards and guidelines (CMS ARS) that address specific information security and privacy requirements
- Procedures (RMH series) that assist in the implementation of the required security and privacy controls based upon the CMS ARS standards.

FISMA further emphasizes the importance of continuously monitoring information system security by requiring agencies to conduct assessments of security controls at a risk-defined frequency. NIST SP 800-53 states under the RA control family that an organization must define, develop, disseminate, review, and update its Risk Assessment documentation at least once every three years. This includes a formal, documented system security package that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and formal, documented processes and procedures to facilitate the implementation of the Risk Assessment policy and associated controls.

The Risk Assessment process exists within the Risk Management Framework (RMF) which emphasizes:

- Building information security capabilities into federal information systems through the application of state-of-the-practice management, operational, and technical security controls
- Maintaining awareness of the security state of information systems on an ongoing basis though enhanced monitoring processes
- Providing essential information to senior leaders to facilitate decisions regarding the mitigation or acceptance of information-systems-related risk to organizational operations and assets, individuals, external organizations, and the Nation.

The RMF[1] has the following characteristics:

- Promotes the concept of near-real-time risk management and ongoing-information-system authorization through the implementation of robust continuous monitoring processes;
- Encourages the use of automation to provide senior leaders the necessary information to make cost-effective, risk-based decisions with regard to the organizational information systems supporting their core missions and business functions;
- Integrates information security and privacy protections into the enterprise architecture and eXpedited Life Cycle (XLC);
- Provides guidance on the selection, implementation, assessment, and monitoring of controls and the authorization of information systems;
- Links risk management processes at the information system level to risk management processes at the organization level through a risk executive (function); and
- Establishes responsibility and accountability for security and privacy controls deployed within organizational information systems and inherited by those systems (i.e., common controls).

[1] https://csrc.nist.gov/publications/detail/sp/800-37/rev-1/final

2. Policy

Policy delineates the security management structure, clearly assigns security responsibilities, and lays the foundation necessary to reliably measure progress, compliance, and direction to all CMS employees, contractors, and any individual who receives authorization to access CMS information technology (IT) systems or systems maintained on behalf of CMS to assure the confidentiality, integrity, and availability of CMS information and information systems.

2.1 Information Systems Security and Privacy Policy (IS2P2)

The CMS IS2P2[2] defines the framework and policy under which CMS protects and controls access to CMS information and information systems in compliance with HHS policy, federal law, and regulations. This Policy requires all CMS stakeholders to implement adequate information security and privacy safeguards to protect all CMS sensitive information.

The policy contained within the CMS IS2P2 and the procedures contained within this document assist in satisfying the requirements for controls that require CMS to create a policy and associated procedures related to Risk Assessment for information systems.

2.2 Chief Information Officer (CIO) Directives

The CMS Chief Information Officer (CIO), the CMS Chief Information Security Officer (CISO), and the CMS Senior Official for Privacy (SOP) jointly develop and maintain the CMS IS2P2. The CIO delegates authority and responsibility to specific organizations and officials within CMS to develop and administer defined aspects of the CMS Information Security and Privacy Program as appropriate.

The dynamic nature of information security and privacy disciplines and the constant need for assessing risk across the CMS environment can cause gaps in policy, to arise outside of the policy review cycle. The CMS Policy Framework includes the option to issue a CIO Directive[3] to address identified gaps in CMS policy and instruction to provide immediate guidance to CMS stakeholders while a policy is being developed, updated, cleared, and approved.

3. Standards

Standards define both functional and assurance requirements within the CMS security and privacy environment. CMS policy is executed with the objective of enabling consistency across the CMS environment. The CMS environment includes users, networks, devices, all software, processes, information in storage or transit, applications, services, and systems that can be connected directly or indirectly to networks. These components are responsible for meeting and complying with the

[2] https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/CMS-Information-Systems-Security-and-Privacy-Policy-IS2P2.html?DLPage=1&DLEntries=10&DLFilter=is2&DLSort=0&DLSortDir=ascending

[3] https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/CIO-Directives-and-Policies/Policies.html

security and privacy baseline defined in policy and further prescribed in standards. The parameters and thresholds for policy implementation are built into the CMS standards, and provide a foundation for the procedural guidance provided by the Risk Management Handbook series.

3.1 Acceptable Risk Safeguards (ARS)

The CMS Acceptable Risk Safeguards (ARS)[4] provides guidance to CMS and its contractors as to the minimum acceptable level of required security and privacy controls that must be implemented to protect CMS's information and information systems, including CMS sensitive information. The initial selection of the appropriate controls is based on control baselines. The initial control baseline is the minimum list of controls required for safeguarding an IT system based on the organizationally identified needs for confidentiality, integrity, and/or availability.

A different baseline exists for each security category (high, moderate, low) as defined by NIST Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems. The ARS provides a catalog of low, moderate, and high controls, in addition to non-mandatory controls outside of the FIPS-199 baseline selection. The ARS, based upon the FIPS 200 and NIST SP 800-53, provides guidance on tailoring controls and enhancements for specific types of missions and business functions, technologies, or environments of operation. Users of the ARS may tailor specific mandatory controls as well as most of the non-mandatory and unselected controls.

4. HIPAA Integration

The HIPAA Security Rule is designed to be flexible, scalable, and technology-neutral, which enables it to be adaptive and seamlessly integrate with detailed frameworks such as FISMA. Though both regulations are governed by different federal agencies, the HIPAA Security Rule only applies to covered entities and their business associates as defined within HIPAA. Implementation of the FISMA requirements helps achieve compliance with the HIPAA Security Rule. HIPAA provides guidance to address the provisions required for the security of health-related information, whereas FISMA presents instructions for the security of the information and the information systems that support these activities.

The following table is a crosswalk of what controls found in this RMH map to specific sections and requirements found in HIPAA.

Risk Assessment (RA) Control	HIPAA Section
Security Categorization (RA-2)	§164.308(a)(7)(ii)(E); §164.308(a)(1)(i); §164.308(a)(1)(ii)(A); §164.308(a)(1)(ii)(B); §164.308(a)(6); §164.308(a)(8); §164.316(a); §164.308(a)(1)(ii)(D); §164.308(a)(7)(ii)(D); §164.316(a)

[4] https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/ARS-31-Publication.html?DLPage=1&DLEntries=10&DLSort=0&DLSortDir=ascending

Risk Assessment (RA-3)	§164.308(a)(1)(i); §164.308(a)(1)(ii)(A); §164.308(a)(1)(ii)(B); §164.308(a)(6); §164.308(a)(7)(ii)(E); §164.308(a)(8); §164.316(a); §164.308(a)(1)(ii)(D); §164.308(a)(7)(ii)(D); §164.308(a)(3); §164.308(a)(4); §164.308(a)(5)(ii)(A); §164.310(a)(1); §164.310(a)(2)(iii); §164.312(a)(1); §164.312(c), §164.312(e); §164.314; §164.316
Vulnerability Scanning (RA-5)	§164.308(a)(1)(ii)(A); §164.308(a)(7)(ii)(E); §164.308(a)(8); §164.310(a)(1); §164.312(a)(1); §164.316(b)(2)(iii); §164.308(a)(1)(i); §164.308(a)(1)(ii)(B); §164.308(a)(5)(ii)(B); §164.308(a)(5)(ii)(C); §164.308(a)(6)(ii); §164.314(a)(2)(i)(C)

5. Roles and Responsibilities

A comprehensive list of information security and privacy roles and responsibilities for CMS stakeholders is contained in the CMS IS2P2. The following roles from the CMS IS2P2 are specific to the procedures contained within this RMH chapter.

Role	Applicable Controls
HHS Chief Information Officer (CIO)	RA-2, RA-3
HHS Chief Information Security Officer (CISO)	RA-3, RA-5(3)
CMS Chief Information Officer (CIO)	RA-2, RA-3
CMS Chief Information Security Officer (CISO)	RA-3, RA-5(3)
CMS Information System Security Officer (ISSO)	RA-2, RA-3, RA-5(1), RA-5(2), RA-5(3), RA-5(4), RA-5(5)
CMS Cyber Risk Advisor (CRA)	RA-2, RA-3
CMS Senior Official for Privacy (SOP)	RA-2, RA-3
CMS Business Owner (BO)	RA-2, RA-3, RA-5(1), RA-5(2), RA-5(3), RA-5(4), RA-5(5)
CMS Federal Employee and Contractors	RA-2, RA-3, RA-5(1), RA-5(2), RA-5(3), RA-5(4), RA-5(5)
CMS Data Guardian (DG)	RA-2
CMS Information System Owner (ISO)	RA-2, RA-3, RA-5, RA-5(2), RA-5(3), RA-5(4)
CMS Privacy Advisor	RA-2, RA-3
CMS Authorizing Official (AO)	RA-2, RA-3

6. Procedures

This section contains the applicable procedures that facilitate the implementation of the RA family security and privacy controls as required by the NIST 800-53A, CMS IS2P2, and the CMS ARS. To increase traceability, each procedure maps to the associated NIST controls using the control number from the CMS IS2P2.

6.1 Security Categorization (RA-2)

Security categories describe the potential adverse impacts to organizational operations, organizational assets, and individuals if organizational information and information systems are compromised through a loss of confidentiality, integrity, and/or availability. Organizations conduct the security categorization process as an organization-wide activity with the involvement of chief information officers, senior information security officers, information system owners, mission/business owners, and information owners/stewards. Security categories are used in conjunction with vulnerability and threat information in assessing the risk to an organization. The security category of an information type can be associated with both user information and system information. Establishing an appropriate security category of an information type requires determining the potential impact level for each security objectives of confidentiality, integrity, and availability (CIA) associated with the particular information type.

SECURITY OBJECTIVE	POTENTIAL IMPACT		
	LOW	MODERATE	HIGH
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Figure 1: Categorization of Federal Information and Information Systems[5]

At CMS, each new system must define its security categorization within the CMS FISMA Controls Tracking System (CFACTS). Before the System Security Plan (SSP) can be developed, the information system and the information resident within that system must be categorized based on the Federal Information Processing Standards Publication 199 (FIPS 199). NIST Special Publication 800-60 Volume I: *Guide for Mapping Types of Information and Information Systems to Security Categories* provides a guideline for mapping types of information and information systems to security categories and works in conjunction with FIPS 199.

The SSP provides the detailed descriptions of all the implemented controls by the CMS ARS categories to minimize risks. Authorization boundaries are also developed and reviewed in correlation with the security categorization as the boundary has a direct effect on the categorization of the system. CMS has synthesized and identified the information types that apply to CMS into 11 information types:

Table 1: CMS Information Types

Information Type	System Security Level	e-Authentication Level
Investigation, intelligence-related, and security information (14 CFR PART 191.5(D))	High	Level 4
Mission Critical Information	High	Level 4
Information About Persons	Moderate	Level 2 or Level 3
Financial, budgetary, commercial, proprietary and trade secret information	Moderate	Level 3
Internal Administration	Moderate	Level 3
Other Federal Agency Information	Moderate	Level 3
New technology controlled scientific information	Moderate	Level 3
Operational Information	Moderate	Level 3
System Configuration Management Information	Moderate	Level 3
Other Sensitive Information	Low	Level 2

[5] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v1r1.pdf

Public Information	Low	None or Level 1

The security categorization for an information system is completed by the Information System Security Officer and approved by the Information System Owner. All CMS information systems categorized as High or Moderate are considered sensitive or contain sensitive information. All CMS information systems categorized as Low are considered non-sensitive or contain non-sensitive information. Organizations implement the minimum security requirements and controls as established in the current CMS Information Security ARS Standard, based on the system security categorization. When identifying information types and assigning appropriate security categorizations for CMS systems, it is essential that the Data Guardian, Information System Owner, Business Owner, Information System Security Officer, and Cyber Risk Advisor coordinate their efforts.

The following steps detail the CMS specific process for conducting a security categorization on an information system using CFACTS:

- **Step 1**: Login to CFACTS and select the "Assessment & Authorization (A&A)" dropdown tab from the top menu.
- **Step 2**: Click on the "Authorization Package - Records" under the "Quick Links" section.
- **Step 3**: Select the appropriate information system. You may also find the information system by clicking on the search icon in the top right of the page and specifying search criteria.
- **Step 4**: Once the information system has been located, click on the system name to open the authorization package for the system.
- **Step 5**: Select the "Security Category" tab from the top navigation tab of the authorization package.
- **Step 6**: Click "Edit" at the top of the authorization package window.
- **Step 7**: Answer the following question in the Organizational Users Section: "Is this system accessed by non-organizational users?"
    1. For help determining who is considered an organizational user and a non-organizational user, see the help text by clicking on the question mark to the left of the question.
- **Step 8**: Select the information types processed, stored or transmitted by the system.
    1. In the Information Type section, click on the right hand side of the "Lookup" title bar in the upper right hand corner.
    2. In the "Record Lookup" pop up, select the checkbox to the left of each information type that is used by your information system.
    3. Click "Ok" when done.
- **Step 9:** Answer the following question in the Personally Identifiable Information (PII) section: "Does this FISMA system collect, maintain, use or share Personally Identifiable Information (PII)?"

- **Step 10:** Answer the following question in the Protected Health Information (PHI) section: "Is the data maintained in this FISMA system considered electronic Protected Health Information (PHI)?"
- **Step 11**: Click "Save" at the top of the screen to save all changes.

The SOP ultimately reviews and approves the categorization of information systems that process, store, or transmit PII.[6]

6.2 Risk Assessment (RA-3)

Risk assessment is the process of identifying risks, both business and technical, to organizational operations' mission, functions, image, and reputation, including individuals, organizational assets, other organizations, and the Nation, resulting from the operation of an information system. As part of risk management, risk assessment incorporates threat and vulnerability analyses and considers mitigations provided by security and privacy controls planned or in place.

This publication focuses on the risk assessment component of risk management—providing a step-by-step process for organizations on: (i) how to prepare for risk assessments; (ii) how to conduct risk assessments; (iii) how to communicate risk assessment results to key organizational personnel; and (iv) how to maintain the risk assessments over time. Risk assessments are not simply one-time activities that provide permanent and definitive information for decision makers to guide and inform responses to information security and privacy risks. Rather, organizations employ risk assessments on an ongoing basis throughout the system development life cycle and across all of the tiers in the risk management hierarchy—with the frequency of the risk assessments and the resources applied during the assessments, commensurate with the expressly defined purpose and scope of the assessments.

6.2.1 Basic Risk Management

Risk assessment is a key component of a holistic, organization-wide risk management process as defined in NIST Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*. Risk management processes include: (i) framing risk; (ii) assessing risk; (iii) responding to risk; and (iv) monitoring risk. Figure 2 illustrates the four steps in the risk management process—including the risk assessment step and the information and communications flows necessary to make the process work effectively.

[6] https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf

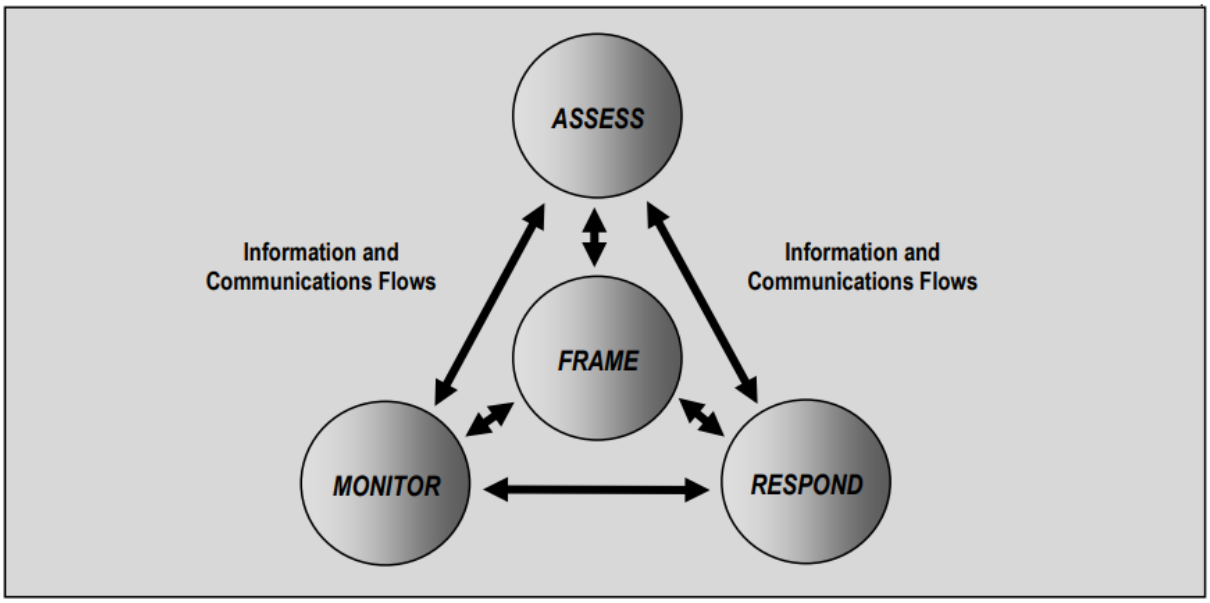


Figure 2: Risk Assessment within the Risk Management Process[7]

As laid out by NIST in 800-30, the first component of risk management addresses how organizations frame risk or establish a risk context—that is, describing the environment in which risk-based decisions are made. The purpose of the risk framing component is to produce a risk management strategy that addresses how organizations intend to assess risk, respond to risk, and monitor risk—making explicit and transparent the risk perceptions that organizations routinely use in making both investment and operational decisions. The risk management strategy establishes a foundation for managing risk and delineates the boundaries for risk-based decisions within organizations.

The second component of risk management addresses how organizations assess risk within the context of the organizational risk frame. The purpose of the risk assessment component is to identify: (i) threats to organizations (i.e., operations, assets, or individuals) or threats directed through organizations against other organizations or the Nation; (ii) vulnerabilities internal and external to organizations; (iii) the harm (i.e., adverse impact) that may occur given the potential for threats exploiting vulnerabilities; and (iv) the likelihood that harm will occur. The end result is a determination of risk (i.e., typically a function of the degree of harm, i.e., impact to the organization, and likelihood of harm occurring).

The third component of risk management addresses how organizations respond to risk once that risk is determined based on the results of a risk assessment. The purpose of the risk response component is to provide a consistent, organization-wide response to risk, or "risk mitigation plan", in accordance with the organizational risk frame by: (i) developing alternative courses of action for responding to risk; (ii) evaluating the alternative courses of action; (iii) determining appropriate courses of action consistent with organizational risk tolerance; and (iv) implementing risk responses based on selected courses of action.

[7] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

The fourth component of risk management addresses how organizations monitor risk over time. The purpose of the risk monitoring component is to: (i) determine the ongoing effectiveness of risk responses (consistent with the organizational risk frame); (ii) identify risk-impacting changes to organizational information systems and the environments in which the systems operate; and (iii) verify that planned risk responses are implemented and information security and privacy requirements derived from and traceable to organizational missions/business functions, federal legislation, directives, regulations, policies, standards, and guidelines are satisfied.

Effective information security and privacy-related risk management is a holistic activity and requires integration of risk input from the information system level (Tier 3) through the organization's business processes (Tier 2) and up through the governance of the enterprise (Tier 1). Risk management among the top and bottom tier are bi-directional as the highest tier directs the lower tiers through policy and processes, and the lower tier feeds tactical risk back up the enterprise. The RMF primarily operates at Tier 3 but does involve interactions in the other two tiers through feedback from ongoing authorization decisions, dissemination of updated threat and risk information to authorizing officials and information system owners.

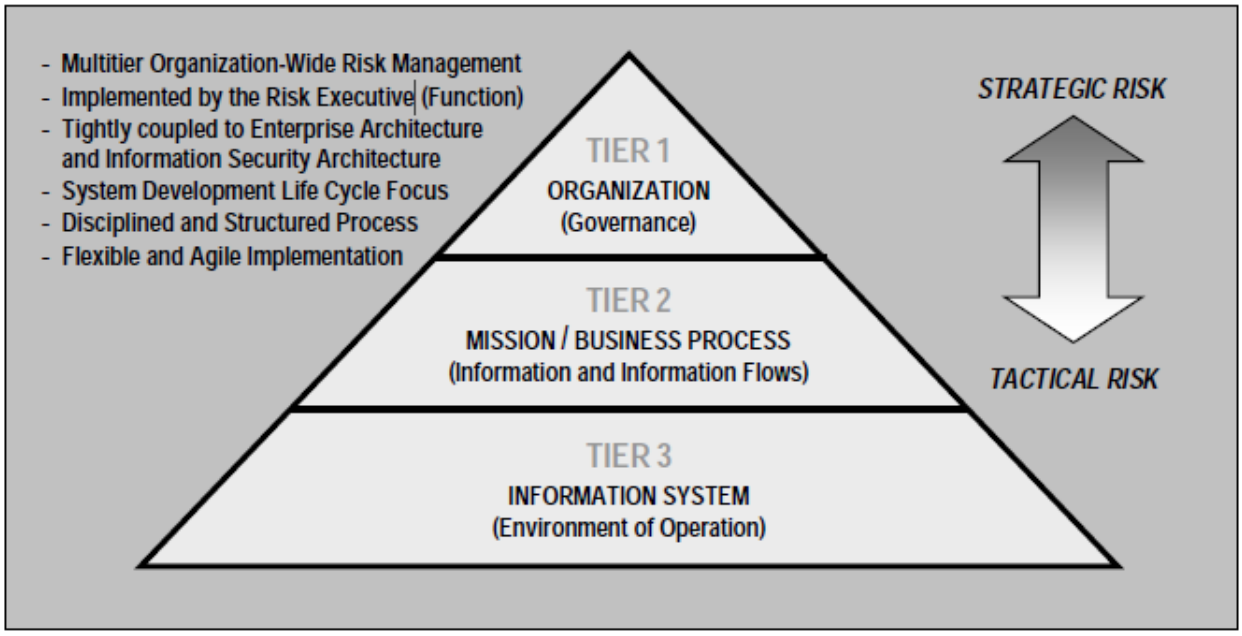


Figure 3: Tiered Risk Management Approach[8]

6.2.2 Risk Models

Risk models define the risk factors to be assessed and the relationships among those factors. Risk factors are characteristics used in risk models as inputs to determining levels of risk in risk assessments. Risk factors are also used extensively in risk communications to highlight what strongly affects the levels of risk in particular situations, circumstances, or contexts. Typical risk factors include threat, vulnerability, impact, likelihood, and predisposing condition. Risk factors

[8] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf

can be decomposed into more detailed characteristics (e.g., threats decomposed into threat sources and threat events). These definitions are important for organizations to document prior to conducting risk assessments because the assessments rely upon well-defined attributes of threats, vulnerabilities, impact, and other risk factors to effectively determine risk.

Figure 4 below illustrates an example of a risk model including the key risk factors discussed above and the relationship among the factors. Each of these risk factors is used in the risk assessment process.

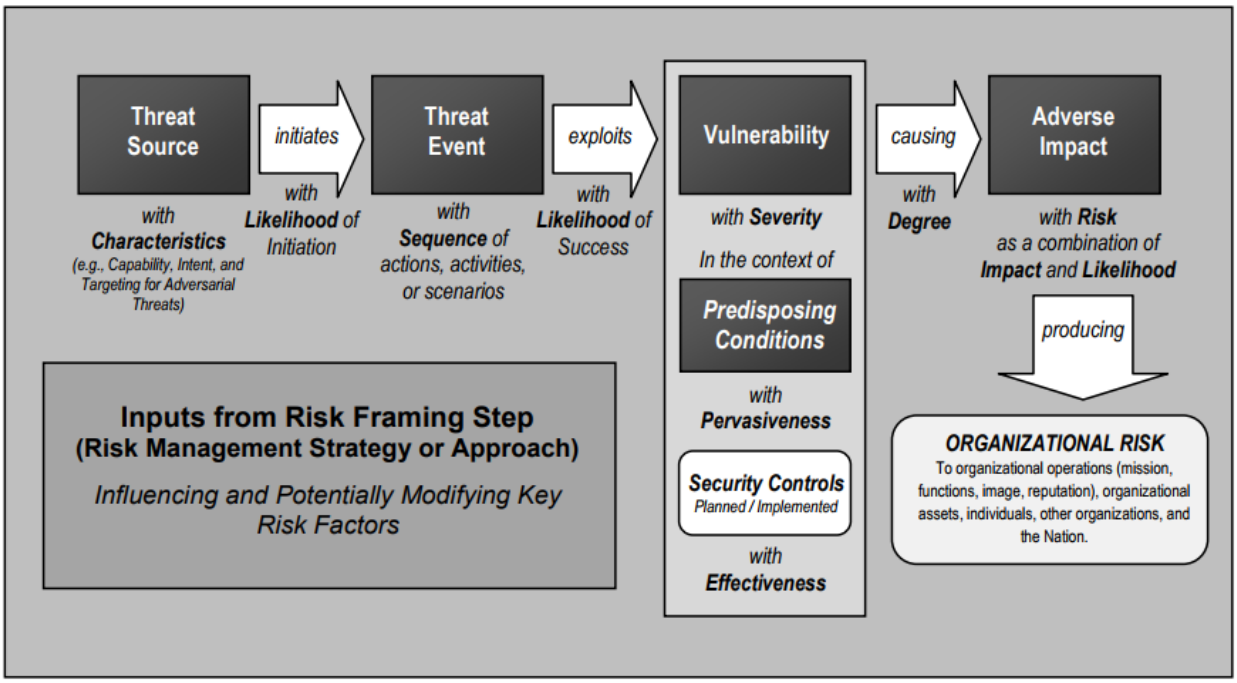


Figure 4: Generic Risk Model with Key Risk Factors[9]

As noted above, risk is a function of the likelihood of a threat event's occurrence and potential adverse impact should the event occur. This definition accommodates many types of adverse impacts at all tiers in the risk management hierarchy described in NIST Special Publication 800-39[10] (e.g., damage to image or reputation of the organization or financial loss at Tier 1; inability to successfully execute a specific mission/business process at Tier 2; or the resources expended in responding to an information system incident at Tier 3). It also accommodates relationships among impacts (e.g., loss of current or future mission/business effectiveness due to the loss of data confidentiality; loss of confidence in critical information due to loss of data or system integrity; or unavailability or degradation of information or information systems). For purposes of risk communication, risk is generally grouped according to the types of adverse impacts and possibly the time frames in which those impacts are likely to be experienced.

[9] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf
[10] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf

6.2.3 High Value Assets

Per OMB Memorandum M-17-09[11] Federal Agencies must extend their risk management approach to include High Value Assets (HVA). HVAs are assets, information systems, information, and data which unauthorized use could cause a significant impact to the United States' national security interests. HVA risk assessments require the agency to incorporate enterprise-wide risk considerations to include operational, business, mission, and continuity. Agencies' assessment of risk should consider not only the risk that an HVA poses to the agency itself, but also the risk of interconnectivity and interdependencies leading to significant adverse impact on the functions, operations, and mission of other agencies. Agencies' assessment of risk to an HVA should be informed by an up-to-date awareness of threat intelligence regarding agencies' Federal information and information systems; the evolving behaviors and interests of malicious actors; and the likelihood that certain agencies and their HVAs are at risk owing to demonstrated adversary interest in agencies' actual, related, or similar assets.[12]

Figure 5: Agency HVA Process Framework[13]

[11] https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-09.pdf
[12] https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-09.pdf
[13] https://policy.cio.gov/hva/process/

There are 7 actions that make up the continuous HVA process:

Plan: Prepare for the HVA process, including stakeholder engagement, governance and oversight, third party engagement, and incorporation of HVA activities into broader agency IT planning.
Identify: Examine systems from the agency's perspective, adversary's perspective, and enterprise-wide perspective to determine those assets which may be considered HVAs.
Categorize: Organize information systems based on (among other things) system function, what kind of and how much information the system contains, the system's importance to the agency's mission, and the scale of impact from system loss or compromise.
Prioritize: Rank HVA systems in terms of risk, considering the categories of threat, vulnerability, and consequence.
Report: Agencies are responsible for keeping their internal HVA lists up-to-date. All CFO Act agencies are required to report their HVAs to DHS on an annual basis.
Assess: The HVA system(s) will be assessed by DHS through a Risk and Vulnerability Assessment (RVA), Security Architecture Review (SAR), and any additional services as deemed necessary.
Remediate: Agencies will receive a detailed report from DHS regarding the HVA system including recommended actions to address the findings.[14]

Risk assessments can also be conducted at various steps in the Risk Management Framework, including categorization, security control selection, security control implementation, security and privacy controls assessment, information system authorization, and security control monitoring. RA-3 is a noteworthy control because it must be partially implemented prior to the implementation of other controls in order to complete the first two steps in the Risk Management Framework.[15] Generally, risk assessments will follow four (4) steps[16]:

[14] https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-09.pdf
[15] https://nvd.nist.gov/800-53/Rev4/control/RA-3
[16] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

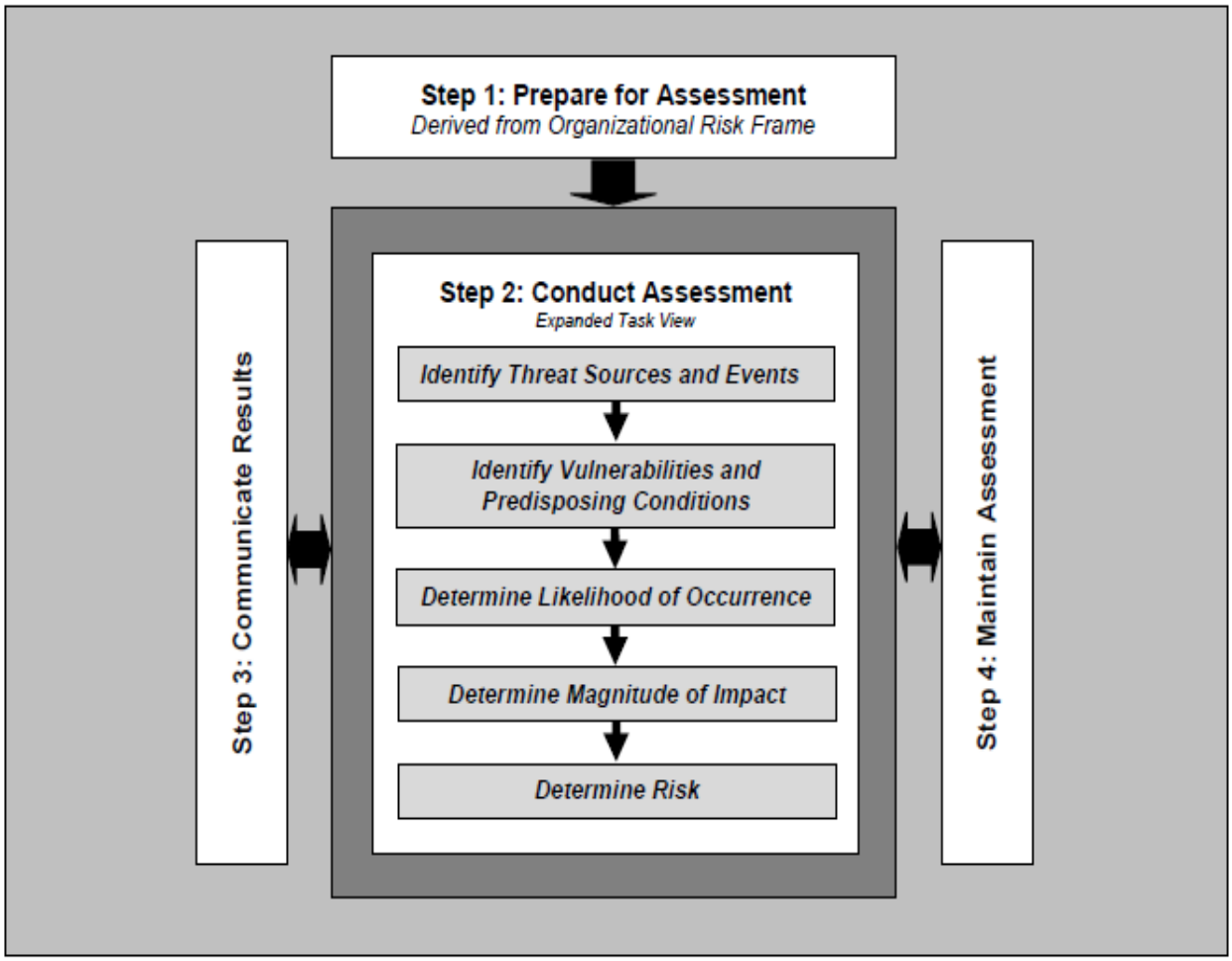


Figure 6: Risk Assessment Process[17]

NIST Special Publication 800-30[18] provides summary guidance on the tasks necessary for each step of the risk assessment process:

Table 2: Summary of Risk Assessment Tasks

Task	Task Description
Step 1: Prepare for Risk Assessment	
Identify purpose of the assessment	Identify the purpose of the risk assessment in terms of the information that the assessment

[17] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf
[18] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

	is intended to produce and the decisions the assessment is intended to support.
Identify the scope of the assessment	Identify the scope of the risk assessment in terms of organizational applicability, time frame supported, and architectural/technology considerations.
Identify assumptions and constraints	Identify the specific assumptions and constraints under which the risk assessment is conducted.
Identify information sources	Identify the sources of descriptive, threat, vulnerability, and impact information to be used in the risk assessment.
Identify risk model and analytic approach	Identify the risk model and analytic approach to be used in the risk assessment.
Step 2: Conduct Risk Assessment	
Identify threat sources[19]	Identify and characterize threat sources of concern, including capability, intent, and targeting characteristics for adversarial threats and range of effects for non-adversarial threats.
Identify threat events[20]	Identify potential threat events, relevance of the events, and the threat sources that could initiate the events.
Identify vulnerabilities and predisposing conditions	Identify vulnerabilities and predisposing conditions that affect the likelihood that threat events of concern result in adverse impacts.
Determine likelihood	Determine the likelihood that threat events of concern result in adverse impacts, considering: (i) the characteristics of the threat sources that could initiate the events; (ii) the vulnerabilities/predisposing conditions identified; and (iii) the organizational susceptibility reflecting the safeguards/countermeasures planned or implemented to impede such events.

[19] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf
[20] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

Determine impact	Determine the adverse impacts from threat events of concern, considering: (i) the characteristics of the threat sources that could initiate the events; (ii) the vulnerabilities/predisposing conditions identified; and (iii) the organizational susceptibility reflecting the safeguards/countermeasures planned or implemented to impede such events.
Determine risk	Determine the risk to the organization from threat events of concern considering: (i) the impact that would result from the events; and (ii) the likelihood of the events occurring.
Step 3: Communicate and Share Risk Assessment Results	
Communicate risk assessment results	Communicate risk assessment results to organizational decision makers to support risk responses. (For CMS this includes Cyber Risk Advisors)
Share risk-related information	Share risk-related information produced during the risk assessment with appropriate organizational personnel.
Step 4: Maintain Risk Assessment	
Monitor risk factors	Conduct ongoing monitoring of the risk factors that contribute to changes in risk.
Update the risk assessment	Update existing risk assessment using the results from ongoing monitoring of risk factors.

Risk Executive (Function)

Risk assessments also can play an important part in determining security control selection, especially when applying tailored guidance. One of the key roles in security control selection, and risk management overall, is the Risk Executive (Function). At CMS, this function is facilitated by the Cyber Risk Advisor (CRA). The CRA is the subject matter expert (SME) in all areas of the CMS Risk Management Framework and as such is responsible for evaluating, maintaining, and communicating the risk posture of each FISMA system to executive leadership, in addition to making risk-based recommendations to the Authorizing Official. CRAs are an invaluable asset to

the risk management process in bridging the lower tier risk environment with that of the higher tier while addressing information security and privacy risk for their FISMA system(s).

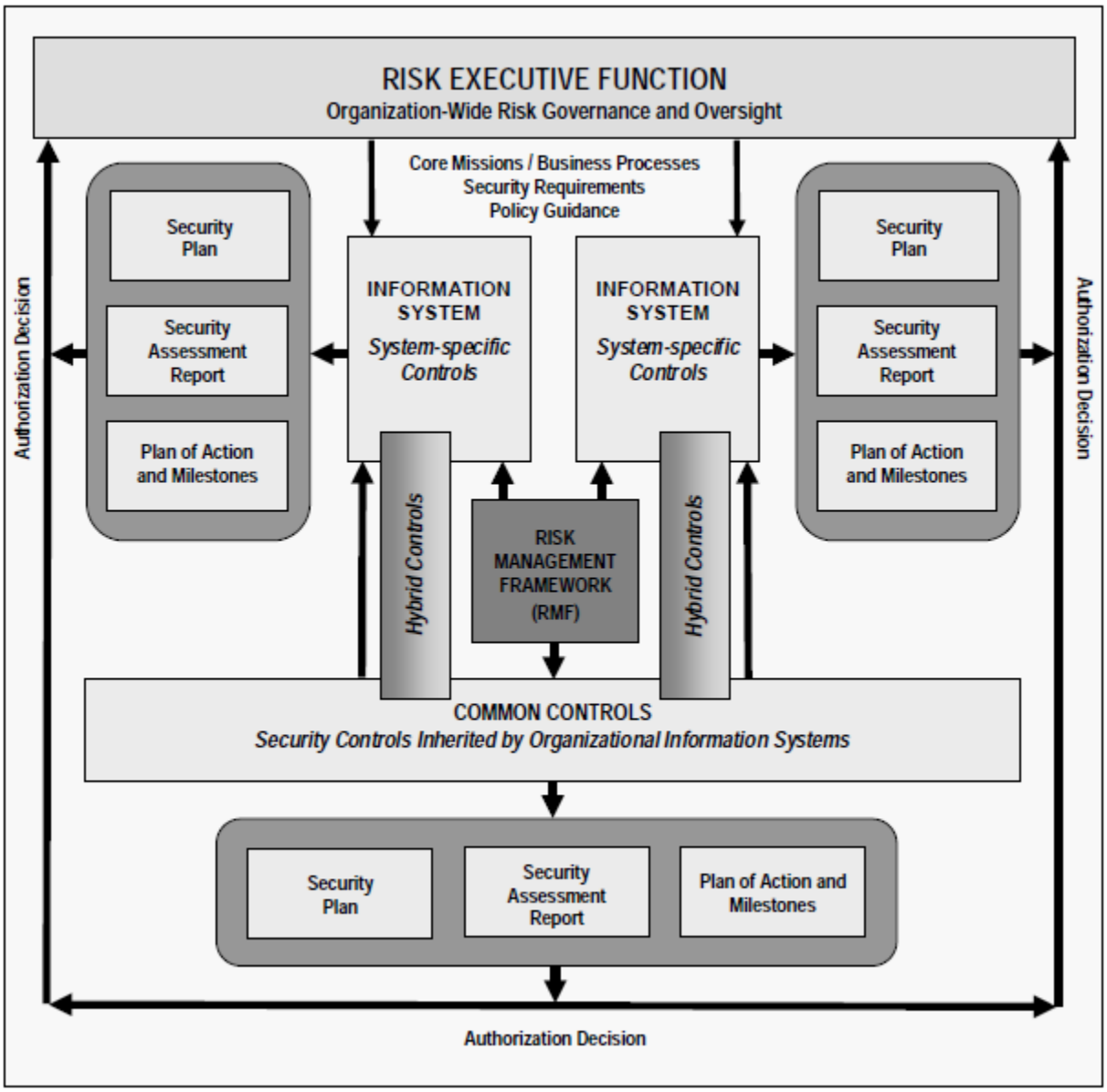


Figure 7: Risk Executive (Function)[21]

The table below outlines the CMS Organizational Defined Parameters (ODPs) for RA-3:

[21] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf

Table 3: CMS Defined Parameters - Control RA-3

Control	Control Requirement	CMS Parameter
RA-3	The organization: b. Documents risk assessment results in [*Selection: security plan; risk assessment report;* [*Assignment: organization-defined document*]]; c. Reviews risk assessment results [*Assignment: organization-defined frequency*]; d. Disseminates risk assessment results to [*Assignment: organization-defined personnel or roles*]; and e. Updates the risk assessment [*Assignment: organization-defined frequency*] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.	The organization: b. [Added] Conducts an e-Authentication Risk Assessment (ERA), as required, on systems and determine e-authentication assurance levels; c. Documents risk assessment results in the applicable security plan; d. Reviews risk assessment results within every 365 days; e. Disseminates risk assessment results to affected stakeholders, Business Owner(s), and the CMS CISO; and f. Updates the risk assessment before issuing a new authority to operate (ATO) package or within every three (3) years, whichever comes first; 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.

Privacy Risk

When considering privacy risks, privacy programs shall consider the risks to an individual or individuals associated with the agency's creation, collection, use, processing, storage, maintenance, dissemination, disclosure, or disposal of their Personal Identifiable Information (PII). Titles II and III of the E-Government Act of 2002 require that agencies evaluate systems that

collect PII and determine whether the privacy of that PII is adequately protected[22]. This evaluation is performed by conducting a Privacy Impact Assessment (PIA)[23]. In order to determine if a PIA is necessary, the Information System Owner (ISO) must conduct a Privacy Threshold Analysis (PTA) to identify any PII within a system. PTAs determine whether a Privacy Impact Assessment (PIA) is required, whether a System of Records Notice (SORN) is required, and if any other privacy requirements apply to the information system. PTAs are usually submitted to an organization's privacy office for review and approval. PTAs are comprised of simple questionnaires that are completed by the System Owner in collaboration with the data owner. PTAs are useful in initiating the communication and collaboration for each system between the privacy officer, the ISO, and the information officer.[24]

A PIA must be conducted under the following circumstances:

- When a PTA indicates that a PIA is required;
- Before developing or procuring IT systems or projects that collect, maintain, or disseminate information in identifiable form;
- When a significant change occurs to a system; or
- Every 3 years for existing systems without changes.

When a significant change occurs to a system, the system's PIA must be updated to reflect how the changes may affect the information. As defined by OMB Memorandum 03-22[25], significant changes include:

- Conversions: Converting paper-based methods to electronic systems, consistent with the Paperwork Reduction Act;
- Anonymous to Non-anonymous: Applying functions to an existing electronic information collection that changes anonymous information into information in identifiable form;
- Significant System Management Changes: When new uses of an existing IT system, including application of new technologies, significantly change the process of managing information in identifiable form in the system;
- Significant Merging: Adopting or altering business processes so that Government databases holding information in identifiable form are merged, centralized, matched with other databases, or otherwise significantly manipulated;
- New Public Access: Applying user-authenticating technology (e.g., password, digital certificate, biometric) to an IT system that can be accessed by the public;

[22] https://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf

[23] HHS guidance on Privacy Impact Assessments can be found here: https://www.hhs.gov/about/agencies/asa/ocio/cybersecurity/pias-and-resources/index.html

[24] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf

[25] https://obamawhitehouse.archives.gov/omb/memoranda_m03-22/

- Commercial Sources: Integrating information in identifiable form obtained from commercial or public sources into an existing information system database;
- New Interagency Uses: When agencies work together on shared functions involving significant new uses or exchanges of information in identifiable form;
- Internal Flow or Collection: When alteration of a business process results in significant new uses or disclosures of information or incorporation into the system of additional information in identifiable form; and
- Alteration in Character of Data: When new information in identifiable form added to an electronic information collection raises the risks to personal privacy, such as the addition of health or privacy information.

Risk Assessment and the CMS Expedited Lifecycle (XLC Framework)

The CMS RA process is initiated during the Concept phase within the CMS Expedited Life Cycle (XLC) Framework. While the Business Owner is responsible for the overall process, it is likely that the Information System Security Officer (ISSO) will perform many of the tasks involved in the Information System Risk Assessment (ISRA) process. Risk activities as related to the XLC phases are as follows:

Phase 1 – Initiation (Intake)

The Business Owner or Information System Security Officer works with the Office of Information Technology Chief Information Security Officer to determine if their system is either a General Support System (GSS) or a Major Application (MA) and what FISMA system family controls will be applied. In addition, the ISSO must determine whether the system will collect, maintain, store, or share PII/PHI. If yes, then the ISSO will coordinate with their corresponding Cyber Risk Advisor and Privacy Expert in conducting a Privacy Threshold Analysis and Privacy Impact Assessment. Once the PIA is completed the CRAs will work together in analyzing the PIA in order to determine the HVA score for the information system. If this HVA score is among the top 10 of systems scored then it is placed on the HVA Tracking List which is overseen by the CMS Senior Official for Privacy (SOP) and provided to HHS upon request[26]. The CMS SOP must ensure that a review of the agency's HVAs is conducted to identify those HVAs that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII. For HVAs identified in the review, the SOP shall ensure that all required privacy documentation and materials are complete, accurate, and up-to-date. CMS must review the following artifacts as part of its review:

· Information System Privacy Plan (SPP), which will be contained within the System Security Plan (SSP)
· System of Records Notice (SORN)
· Privacy Act Statements
· Privacy Impact Assessment (PIA)

[26] CMS utilizes the OMB Max Portal in providing monthly vulnerability scans and CMS HVA inventory on a quarterly basis

For systems that utilize remote authentication of individuals over a network, an ERA must be performed. Guidance on conducting an ERA can be found in the NIST 800-63 suite[27]. Also, CMS provides the associated System Security Level and e-Authentication Levels along with its information types in Table 1.

Once the BO or ISSO obtains the designation, the identification of the System Security Level by Information Type is determined. Upon establishing these levels, the ISSO will review the CMS ARS for the level of controls that must be employed by the system. For additional guidance, reference CMS document: "Process for Determining E-Authentication Levels for CMS Systems"

Phase 2 – Concept

The BO or ISSO begins to identify business risks, and the initial draft of the ISRA is developed. While this phase begins the ISRA process, subsequent phases will require updates to the ISRA. The business risks during this phase are defined as the vulnerabilities and threats that could be exploited and result in the loss of business functionality.

Phase 3 – Planning

The BO or ISSO reviews the minimum level of security and privacy controls contained in the CMS ARS and performs an evaluation of the controls to determine the appropriate level of controls for their system. The ISSO will document the expected minimum controls relative to the sensitivity level of the system as defined in the CMS ARS. Identified risks are used to support the development of the system requirements, including security requirements, and a security concept of operations.

Phase 4 – Requirements Analysis

The BO or ISSO begins developing the SSP during this phase, while continuing the ISRA process. CFACTS provides an auto-generated template to be used when writing the system SSP, under the "Authorization" tab when looking in a system's authorization package. Also, guidance on developing an SSP is provided by RMH Chapter 12 Security and Privacy Planning[28].

Phase 5 – Design

The BO or ISSO updates the ISRA during this phase to account for any risks, vulnerabilities, and/or safeguards that have been identified or changed. The SSP, which contains the detailed descriptions of controls that are in place for the system to ensure CIA, must also be updated as needed during this phase. In addition, the system requirements must capture the business and

[27] https://www.nist.gov/itl/tig/projects/special-publication-800-63

[28] https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/RMH-Chapter-12-Security-and-Privacy-Planning.html

security risks, as applicable, and translate them into the effective system design to protect the CIA of the CMS system. The risks identified during this phase can be used to support the security analyses of the IT system that may lead to architecture and design tradeoffs during system development.

Phase 6 – Development

It is essential that the BO or ISSO update the ISRA during this phase to account for any risks, vulnerabilities, and safeguards that have been identified or changed as the development phase progresses.

Phase 7 – Test

During the testing phase, the BO or ISSO shall identify an independent organization to conduct a Security Assessment based on the ISRA and accompanying SSP. The purpose of the Security Assessment is to test the effectiveness of the security and privacy controls of the system as they have been applied in an operational environment. The objective is to verify that the applied controls operate as defined, meet the approved security and privacy specification for the software and hardware, and implement the organization's security requirement. Decisions regarding identified risks must be made prior to system operation and are reviewed by the SOP to ensure compliance with applicable privacy requirements. In addition to the security artifacts produced during this phase, the finalized and approved PIA takes place in this phase.

Phase 8 – Implementation

The ISRA and SSP will be finalized and incorporated into the Authority to Operate (ATO) submission package. Once this is done, the ISSO will submit the package to the CIO through the CISO. The CIO may provide a signed system authorization or deny operation of the system until certain corrective actions are taken. Controls that need to be resolved will require a Plan of Action and Milestones (POA&M) which is covered in detail in RMH Chapter 4: Security Assessment and Authorization, Control CA-5.[29]In addition more detailed information regarding POA&Ms can be found in Appendix G.

Phase 9 – Operations and Maintenance

During this phase, the BO or ISSO will continue to update the ISRA as needed and shall conduct annual security assessment and Contingency Plan (CP) testing on an annual basis. All identified risks or findings must be used in updating the ISRA. If there are changes in the system that affect security then a Security Impact Analysis (SIA) must be performed[30]. Other risk management

[29] RMH Chapter 4: Security Assessment and Authorization: https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html

[30] RMH Chapter 5: Configuration Management: https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html

activities also take place during this phase to include mitigating system weaknesses through POA&Ms.

Phase 10 – Disposition Phase

During this phase, the system and components are archived and must be maintained for three (3) years after the system is declared retired. The BO or ISSO shall continue to update the ISRA as needed to reflect changes in the environment of the system.

CMS requires the BO or ISSO to develop or update an ISRA in response to each of the following events:

- New system;
- Major business process or technology/system modification(s);
- Every third year of an operational system;
- Before submittal of a new ATO package;
- Increase in security risks/exposure;
- Increase of overall system security level; and/or,
- Serious security violation(s) as described in the CMS Risk Management Handbook Chapter 8 Incident Response[31].

Risk assessment information is managed through CMS Federal Information Security Management Act Controls Tracking System (CFACTS). Follow the steps provided below to manage the Information System Risk Assessment (ISRA) for a system in CFACTS:

- **Step 1:** The ISSO or support contractor creates an ISRA in CFACTS using the subtasks below:
    1. Login to CFACTS and select the *"Assessment & Authorization (A&A)"* tab from the top menu.
    2. Click on "Authorization Package – Records" under the "Quick Links" column and select the appropriate information system from the list. You may also find the information system by clicking *"Search Records"* and specifying search criteria.
    3. Once the information system has been located, click on the system name to open the authorization package for the system.
    4. Select the *"Security Category"* tab from the top navigation tab of the authorization package.
    5. Scroll down to the *"ISRA"* tab located at the bottom of the page and click on it.
    6. Click on the "Add New" link to the right of the page. This should prompt generation of the Information System Risk Assessment (ISRA) Template such as the one provided in Appendix D.

[31] https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/RMH-Chapter-08-Incident-Response.pdf

- **Step 2:** The ISSO or contractor support staff provide their assessor(s) with the ISRA template for them to fill out upon completion of the assessment.
- **Step 3:** The assessor(s) will submit the ISRA to the ISSO upon completion of the security assessment.
- **Step 4:** The ISSO will continue to update the ISRA on an as needed basis. The ISSO must use the ISRA located in CFACTS by updating it and uploading a new version reflecting the date of approval for each update.

Risk Acceptance

Risk acceptance is a common and appropriate practice within an organization. When the risk response with the identified risk is within the organization's risk tolerance and/or the risk has been sufficiently mitigated to an acceptable level, the organization may choose to accept the risk. Risk deemed to be low, moderate, or high can be accepted depending on particular situations or conditions which are unique to the organization. For example, organizations with data centers residing in the northeastern portion of the United States may opt to accept the risk of earthquakes based on known likelihood of earthquakes and data center vulnerability to damage by earthquakes. Organizations accept the fact that earthquakes are possible, but given the infrequency of major earthquakes in that region of the country, believe it is not cost-effective to address such risk—that is, the organizations have determined that risk associated with earthquakes is low, due to the likelihood of a non-occurrence, and therefore acceptable. Conversely, organizations may accept substantially greater risk (in the moderate/high range) due to compelling mission, business, or operational needs. Organizations typically make determinations regarding the general level of acceptable risk and the types of acceptable risk with consideration of organizational priorities and trade-offs between: (i) near-term mission/business needs and potential for longer-term mission/business impacts; and (ii) organizational interests and the potential impacts on assets such as individuals and information systems.[32] Some scenarios requiring a Risk Acceptance are:

- When the cost of implementing the control is more than the benefit gained
- When implementation of the control results in adverse effects to functionality of the system
- It is technically infeasible to implement the control
- When implementing the control results in disrupting the business process

This list is by no means exhausting and is intended to provide some of the most common scenarios for Risk Acceptance.

Due to the nature of a risk being accepted by an organization, the responsibility cannot be delegated to just any official. Instead, the responsibility is given to the Authorizing Official (AO) in making the final decision on risk acceptance for a system.

When a CMS system is non-compliant with a CMS policy, standard, or other security requirement and is unable to remediate the issue within the POA&M process, a risk acceptance request must be submitted to the CIO. The CMS Information Security Policy/Standard Risk Acceptance template can be found in Appendix E. This is part of the Risk Based Decisions (RBD) process and

[32] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf

is documented in CFACTS for CMS systems. Follow the steps provided below to create a risk acceptance for a system in CFACTS:

- **Step 1:** The Information System Security Officer (ISSO) or support contractor creates a Risk Acceptance in CFACTS using the subtasks below:
    1. Login to CFACTS and select the *"Assessment & Authorization (A&A)"* tab from the top menu.
    2. Click on "*POA&Ms – Records*" under the "*Quick Links*" column and select the appropriate POA&M ID from the list. You may also find the POA&M ID by clicking *"Search Records"* and specifying search criteria.
    3. Once the POA&M ID has been located, click on the POA&M ID to open the detailed view of the weakness.
    4. Select the *"Related Risk Acceptance (RBD)"* tab from the middle of the interface.
    5. Click on the "*Add New*" link to the right of the "*Related Risk Acceptance (RBD)*" tab to open a risk acceptance.
- **Step 2:** The ISSO or support contractor will work with their CRA in filling out the CMS Information Security Policy/Standard Risk Acceptance form.
- **Step 3:** Once the Risk Acceptance form is completed, the CRA will review it and then update the status in CFACTS under "*General Information*" on the "*Risk Acceptance (RBD)"* interface.
- **Step 4:** Once the Risk Acceptance is approved, the ISSO or support contractor will export the form in order to gather the appropriate signatures by clicking on the "*Generate Risk Acceptance Form*" tab under "*Submitter Attachments*" at the bottom of the interface.
- **Step 5:** After gathering the appropriate stakeholder signatures, the ISSO or support contractor will upload the scanned Risk Acceptance into CFACTS by clicking "*Add New"* tab to the right of the "*Submitter Attachments"* tab.
- **Step 6:** After the Risk Acceptance is uploaded, it will be reviewed for final approval by the CISO.

6.3 Vulnerability Scanning (RA-5)

A vulnerability is a weakness that can be accidentally triggered or intentionally exploited, usually due to misconfigurations. Vulnerability scanning is a non-destructive form of testing that provides an organized approach to the testing, identification, analysis and reporting of potential security issues on a network. Vulnerability scanners can be run against a host either locally or from the network. Some network-based scanners have administrator-level credentials on individual hosts and can extract vulnerability information from hosts using those credentials. Other network-based scanners do not have such credentials and must rely on conducting scanning of networks to locate hosts and then scan those hosts for vulnerabilities. In such cases, network-based scanning is primarily used to perform network discovery and identify open ports and related vulnerabilities. Network-based scanning without host credentials can be performed both internally and externally—and although internal scanning usually uncovers more vulnerabilities than external scanning, testing from both viewpoints is important. External scanning must contend with perimeter security devices that block traffic, limiting assessors to scanning only the ports authorized to pass traffic.

For local vulnerability scanning, a scanner is installed on each host to be scanned. This is done primarily to identify host Operating Systems (OS) and application misconfigurations and vulnerabilities—both network-exploitable and locally exploitable. Local scanning is able to detect vulnerabilities with a higher level of detail than network-based scanning because local scanning usually requires both host (local) access and a root or administrative account. Some scanners also offer the capability of repairing local misconfigurations.[33]

The foundation for effective vulnerability scanning includes having an asset inventory management process (e.g. automated tools and their processes) in place. Without a robust asset inventory management process in place there is an increased risk that the asset inventory is incomplete which may impact downstream processes to include vulnerability scanning and security configuration. This may lead to vulnerabilities and misconfigurations going unidentified and may result in exploitable conditions.

The results from a vulnerability scan can show the path an adversary can take once they have gained access to the network and how much data they could collect. Vulnerability scans can also support penetration testing (CA-8) by providing information on targets for the penetration testing team to look into. Some examples of scanning activities are:
(i) scanning for patch levels;
(ii) scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and
(iii) scanning for improperly configured or incorrectly operating information flow control mechanisms. Based on the information provided, the organization can then remediate vulnerabilities identified and work towards improving the security of the network.

For CMS, the security categorization of information systems guides the frequency and comprehensiveness of vulnerability scans. All data centers must have a vulnerability scanner in place before connecting to the CMS network, either through their own vendor-provided scanner or by establishing a connection with the Continuous Diagnostics and Mitigation (CDM) team at the CMS Cybersecurity Integration Center (CCIC). One of the services provided by the CCIC includes vulnerability scanning, with support in place for all scanning needed from infrastructure to endpoint[34]. The CCIC supports risk analysis at CMS by ingesting scan logs and identifying risks through its Security Incident Event Management (SIEM) tool. In order to set up vulnerability scanning for new systems, please send an email to the CDM Manager using this email address: EVM-CMP@cms.hhs.gov.

[33] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

[34] A list of CCIC services and descriptions can be found here: https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/CIO-Directives-and-Policies/CIO-IT-Policy-Library-Items/TRA-Volume-II-%E2%80%93-Network-Services.html?DLPage=1&DLEntries=10&DLFilter=volume&DLSort=0&DLSortDir=ascending

If a datacenter chooses not to utilize the vulnerability scanning service provided by the CCIC then they are able to choose a vendor-provided one. There are requirements that must be met for those System Owners who decide not to use the CCIC. These requirements include the baseline configurations that must be scanned against, such as those found in *Risk Management Handbook Chapter 5 Configuration Management*[35] (CM-6). Information for meeting these requirements are found in the *CMS CCIC Integration Requirements* document. For access to this document, please reach out to the CDM Manager by sending an email to: EVM-CMP@cms.hhs.gov.

When vulnerabilities are discovered they must be mitigated within a given timeframe. This timeframe varies depending on the criticality of the vulnerability:

- Critical vulnerabilities within **30 days** from discovery
- High vulnerabilities within **60 days** from discovery
- Medium vulnerabilities within **90 days** from discovery
- Low vulnerabilities within **180 days** from discovery

If the identified vulnerabilities cannot be mitigated within the given time frame and exceed those thresholds then they must be documented in the designated POA&M as weaknesses and mitigated through timelines defined for the corresponding level of weakness.

The table below outlines the CMS ODPs for RA-5:

Table 4: CMS Defined Parameters – Control RA-5

Control	Control Requirement	CMS Parameter
RA-5	The organization: a. Scans for vulnerabilities in the information system and hosted applications [*Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process*] and when new vulnerabilities potentially affecting the system/applications are identified and reported; b. Employs vulnerability scanning tools and techniques that facilitate interoperability among	The organization: a. Scans for vulnerabilities in the information system and hosted applications no less often than once every 72 hours and when new vulnerabilities potentially affecting the system/applications are identified and reported; b. Complies with DHS Continuous Diagnostics and Mitigation program and CMS requirements; and 5.

[35] https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html

Control	Control Requirement	CMS Parameter
	tools and automate parts of the vulnerability management process by using standards for: 1. Enumerating platforms, software flaws, and improper configurations; 2. Formatting checklists and test procedures; and 3. Measuring vulnerability impact; c. Analyzes vulnerability scan reports and results from security control assessments; d. Remediates legitimate vulnerabilities [*Assignment: organization-defined response times*] in accordance with an organizational assessment of risk; and e. Shares information obtained from the vulnerability scanning process and security control assessments with [*Assignment: organization-defined personnel or roles*] to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).	Complying with required reporting metrics (e.g., CyberScope). d. Remediates legitimate vulnerabilities based on the Business Owner's risk prioritization in accordance with the guidance defined under security control SI-02; and e. Shares information obtained from the vulnerability scanning process and security control assessments with affected/related stakeholders on a "need to know" basis to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies)

6.3.1 Update Tool Capability (RA-5(1))

The purpose of this control is to ensure that CMS has the capability to update the scanning tools it uses for vulnerability scanning efforts. New vulnerabilities are a constant and it is essential to update the capability of the tools used as new vulnerabilities are discovered, announced, and published. Better scanning methods are therefore developed in response to the ever-changing threat landscape. As new updates and versions of the vulnerability scanning tools become available, they must be updated in order to ensure that the latest capabilities are deployed in scanning the CMS network. Vendor-provided tools will include a process to update as agreed between the vendor and datacenter.

6.3.2 Update Frequency/Prior to New Scan/When Identified (RA-5(2))

The purpose of this control is to ensure that CMS is updating the vulnerabilities it is scanning for on a regular basis through a defined frequency, prior to each new scan, and when identified. Readily updating the vulnerabilities that are scanned helps to ensure that potential vulnerabilities in the information system are identified and addressed as quickly as possible.

The table below outlines the CMS ODPs for updating the information system vulnerabilities:

Table 5: CMS Defined Parameters – Control RA-5(2)

Control	Control Requirement	CMS Parameter
RA-5(2)	The organization updates the information system vulnerabilities scanned [Selection (one or more): [Assignment: organization-defined frequency]; prior to a new scan; when new vulnerabilities are identified and reported].	The organization updates the database of known information system vulnerabilities to be used in the scanning process no less often than every 72 hours, immediately prior to a new scan, and when new vulnerabilities are identified and reported.

System Owners whose systems are not covered by the CCIC must provide documentation to demonstrate their vendor-provided tools are updated no less often once every 72 hours, immediately prior to a new scan, and when new vulnerabilities are identified and reported.

6.3.3 Discoverable Information (RA-5(4))

The purpose of this control is to ensure that CMS is determining the information that potential adversaries can discover in the event of malicious activities against the CMS network. In addition, this control requires that corrective actions are identified and then taken to eliminate the information discoverable to adversaries. In order to ensure that vulnerability scans are prompting appropriate corrective actions, organizations must be able to determine what information is discoverable by adversaries. For systems that are scanned by the CCIC, the CDM team utilizes a Security Intelligence Hub (SIH) that acts as a central repository of vulnerability information and holds such data specific to that scan for one (1) year. Included in this information are corrective actions that the ISSO can take to remedy the identified vulnerabilities in their systems. The ISSO may request access to this repository by sending an email to the CDM Manager at: EVM-CMP@cms.hhs.gov.

System Owners whose systems are not scanned by the CCIC must provide documentation to the CDM team detailing the information discoverable on their systems to adversaries. This can be done by performing annual searches of common internet locations to find out what information is available on the internet about your system. The procedures for documenting this discoverable information should follow the basic who, what, when, where, and why format. Once this information is determined and documented, the Division of Cyber Threat and Security Operations,

System Owner, and Contractor Staff will establish a meeting to identify and carry out the appropriate corrective actions.

The table below outlines the CMS ODPs for RA-5(4):

Table 6: CMS Defined Parameters – Control RA-5(4)

Control	Control Requirement	CMS Parameter
RA-5(4)	The organization determines what information about the information system is discoverable by adversaries and subsequently takes [Assignment: organization-defined corrective actions].	The organization determines what information about the information system is discoverable by adversaries, and subsequently takes appropriate corrective actions to limit discoverable system information.

6.3.4 Privileged Access (RA-5(5))

There are systems on the CMS network that require privileged access. In order to conduct vulnerability scans on these systems, there must be an ability for the scanners to receive privileged access to these systems. A complete analysis of the privileged areas of system appliances cannot be performed without the necessary privileged access. The purpose of this control is to ensure that CMS identifies the information system components that require privileged access and the vulnerability scanning activities that require such access, as well as ensuring that privileged access is implemented for these activities.

The table below outlines the CMS ODPs for RA-5(5):

Table 7: CMS Defined Parameters – Control RA-5(5)

Control	Control Requirement	CMS Parameter
RA-5(5)	The information system implements privileged access authorization to [Assignment: organization-identified information system components] for selected [Assignment: organization-defined vulnerability scanning activities].	The information system implements privileged access authorization to operating system, telecommunications, and configuration components for selected vulnerability scanning activities to facilitate more thorough scanning.

This can be achieved by obtaining appropriate management approval to allow privileged users such as Firewall Privileged Users and Intrusion Detection Privileged Users to perform vulnerability assessment from the privileged accounts perspective.

Appendix A. Acronyms

Selected acronyms used in this document are defined below.

Acronyms	Terms
AO	Authorizing Official
ARS	Acceptable Risk Safeguards
ATO	Authority To Operate
BAT	Breach Analysis Team
CBT	Computer-based Training
CCIC	CMS Cybersecurity Integration Center
CDM	Continuous Diagnostics and Mitigation
CIA	Confidentiality, Integrity, Availability
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMS	Centers for Medicare & Medicaid Services
CMS CO	CMS Contracting Officers
CMS IS2P2	CMS Information Systems Security and Privacy Policy
CONOPS	Concept of Operations
CRA	Cyber Risk Advisor
CSIRC	Computer Security Incident Response Center
CSIRTs	Computer Security Incident Response Teams
DDoS	Distributed Denial of Service
DoS	Denial of Service
ERS	Enterprise Remedy System
EUA	Enterprise User Administration
FAQ	Frequently Asked Questions

Acronyms	Terms
FISMA 2014	Federal Information Security Modernization Act of 2014
FMAT	Forensics and Malware Analysis Team
FTI	Federal Tax Information
HHS	Department of Health and Human Services
HHS CSIRC	HHS Computer Security Incident Response Center
HIPAA	Health Insurance Portability and Accountability Act of 1996
IDPS	Intrusion Detection and Prevention System
IDS	Intrusion Detection System
IIR	Initial Incident Reporting
IMT	Incident Management Team
IOC	Indicator of Compromise
IP	Internet Protocol
IPS	Intrusion Prevention System
IR	Incident Response
IRA	Incident Response Authority
IRC	Internal Revenue Code
IRL	Incident Response Lead
IRP	Incident Response Plan
IRS	Internal Revenue Service
IRT	Incident Response Team
ISO	Information Systems Owners
ISP	Information Security Personnel
ISPG	Information Security and Privacy Group
ISSO	Information Systems Security Officer
IT	Information Technology

Acronyms	Terms
LAN	Local Area Network
LEOs	Law Enforcement Organizations
NCP	National Checklist Program
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
NVD	National Vulnerability Database
O&M	Operations and Maintenance
OMB	Office of Management and Budget
ODP	Organization-Defined Parameters
OPDIV	Operating Divisions
OS	Operating System
OSSM	OCISO Systems Security Management
OSSO	Office of Security and Support Operation
PCII	Protected Critical Infrastructure Information
PHI	Protected Health Information
PI	Program Integrity
PII	Personally Identifiable Information
PIRT	Privacy Incident Response Team
PIV	Personal Identity Verification
POA&Ms	Plan of Action and Milestones
POC	Point of Contact
Pre-BAT	Pre-Breach Analysis Team
RMH	Risk Management Handbook
SCA	Security Controls Assessment
SCAP	Security Content Automation Protocol

Acronyms	Terms
SIEMs	Security Information Event Management
SDLC	System Development Life Cycle
SOC	Security Operations Center
SOP	Senior Official for Privacy
SP	Special Publication
SQL	Structured Query Language
SSN	Social Security Number
SSP	System Security Plan
SU	System User
SUID	Set User ID
TCP	Transmission Control Protocol
TIGTA	Treasury Inspector General for Tax Administration
TTL	Time to Live
UID	User ID
URL	Universal Resource Locator
USB	Universal Serial Bus
US-CERT	United States Computer Emergency Readiness Team
USGCB	U.S. Government Configuration Baselines
VPN	Virtual Private Network
XLC	Expedited Life Cycle

Appendix B. Glossary of Terms

Selected terms and definitions in this document are defined below (e.g. Breach and a brief definition of its meaning).

Terms	Definitions
Acceptable Risk Safeguards	CMS Information Security Acceptable Risk Safeguards (ARS), CMS Minimum Security Requirements (CMSR),” http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity.
Administrative Vulnerability	An administrative vulnerability is a security weakness caused by incorrect or inadequate implementation of a system’s existing security features by the system administrator, security officer, or users. An administrative vulnerability is not the result of a design deficiency. It is characterized by the fact that the full correction of the vulnerability is possible through a change in the implementation of the system or the establishment of a special administrative or security procedure for the system administrators and users. Poor passwords and inadequately maintained systems are the leading causes of this type of vulnerability.
After Action Report	A document containing findings and recommendations from an exercise or a test.
Authorizing Official	Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals.
Breach	A breach is the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic.
Breach Analysis Team	An information security and privacy incident and breach response team with the capability that includes preparation, identification, containment, eradication, recovery, and follow-up capabilities to ensure effective recovery from information security and privacy incidents and breaches.
Centers for Medicare & Medicaid Services	CMS covers 100 million people through Medicare, Medicaid, the Children's Health Insurance Program, and the Health Insurance Marketplace.
Chief Information Officer	1. Agency official responsible for: • Providing advice and other assistance to the head of the executive agency and other senior management personnel of the agency to ensure that information technology is acquired and information resources are managed in a manner that is consistent

Terms	Definitions
	with laws, Executive Orders, directives, policies, regulations, and priorities established by the head of the agency; • Developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the agency; and • Promoting the effective and efficient design and operation of all major information resources management processes for the agency, including improvements to work processes of the agency
Chief Information Security Officer	The incumbent in the position entitled Chief Information Security Officer. The CISO must be an agency official (federal government employee) and must fulfill all of the responsibilities identified in the HHS IS2P Appendix A Section 11, OpDiv CISOs. The CISO carries out the CIO's information security responsibilities under federal requirements in conjunction with the SOP.
CMS Cybersecurity Integration Center	The CCIC monitors, detects, and isolates information security and privacy incidents and breaches across the CMS enterprise IT environment. The CCIC provides continual situational awareness of the risks associated with CMS data and information systems throughout CMS. The CCIC also provides timely, accurate, and meaningful reporting across the technical, operational, and executive spectrum.
CMS FISMA Controls Tracking System	CMS database that maintains current FISMA information (e.g., POCs, artifacts) to support organizational requirements and processes (e.g., communication, contingency planning, training, data calls).
CMS Minimum Security Requirements	Description of the minimum requirements necessary for an information system to maintain an acceptable level of security.
CMS IT Service Desk	For the purposes of incident response coordination, the CMS IT Service Desk is a sub-component of the CMS Information Security and Privacy Group and IMT, whose responsibilities include but are not limited to the following: • Act as the first point of contact for security incidents or anomalies, and record information provided by the system user, CMS Business Owner (BO)/Information Systems Owner (ISOs) or On-site Incident Response Authority (IRA) , depending on alert source • Generate a CMS incident ticket to document the incident for CMS records • Determine if the incident relates to PII • Immediately refer information security incidents to the IMT
CMS Marketplace	The Affordable Care Act helps create a competitive private health insurance market through the creation of Health Insurance Marketplaces. These State-based, competitive marketplaces, which launch in 2014, will provide millions of Americans and small businesses with "one-stop shopping" for affordable coverage.

Terms	Definitions
Cyber Risk Advisor	Act as Subject Matter Expert in all areas of the CMS Risk Management Framework (RMF).
Department of Health and Human Services	The United States Department of Health and Human Services (HHS), also known as the Health Department, is a cabinet-level department of the U.S. federal government with the goal of protecting the health of all Americans and providing essential human services. Its motto is "Improving the health, safety, and well-being of America". Before the separate federal Department of Education was created in 1979, it was called the Department of Health, Education, and Welfare (HEW).
Data Compromise and Data Spills	Data compromise is the exposure of information to a person not authorized to access that information either through clearance level or formal authorization. This could happen when a person accesses a system he is not authorized to access or through a data spill. Data spill is the release of information to another system or person not authorized to access that information, even though the person is authorized to access the system on which the data was released. This can occur through the loss of control, improper storage, improper classification, or improper escorting of media, computer equipment (with memory), and computer generated output.
Data Destruction or Corruption	The loss of data integrity can take many forms including changing permissions on files so that files are writable by non-privileged users, deleting data files and or programs, changing audit files to cover-up an intrusion, changing configuration files that determine how and what data is stored and ingesting information from other sources that may be corrupt.
Denial of Service (DoS)	An action (or series of actions) that prevents any part of a system from functioning in accordance with its intended purpose. This includes any action that causes unauthorized destruction, modification, delay, or interruption of service. An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources.
Enterprise User Administration	Manages the CMS user identifications. For more detail see https://portal.cms.gov/wps/portal/unauthportal/faq
Event	An event is any observable occurrence in a system or network. Events include a user connecting to a file share, a server receiving a request for a web page, a user sending email, and a firewall blocking a connection attempt. Adverse events are events with a negative consequence, such as system crashes, packet floods, unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malware that destroys data.
Exercise	A simulation of an emergency designed to validate the viability of one or more aspects of an IT plan.

Terms	Definitions
Exercise Briefing	Material that is presented to participants during an exercise to outline the exercise's agenda, objectives, scenario, and other relevant information.
eXpedited Life Cycle	CMS-XLC-1 The CISO must integrate information security and privacy into the CMS life cycle processes. The XLC provides the processes and practices of the CMS system development life cycle in accordance with the CMS Policy for Information Technology (IT) Investment Management & Governance. The CMS CISO maintains the RMH Volume 1 Chapter 1, Risk Management, in the XLC to document the CMS information system life cycle, in accordance with the RMF.
Federal Tax Information (FTI)	Federal Tax Returns and return information are confidential, as required by Internal Revenue Code (IRC) Section 6103. The information is used by the Internal Revenue Service (IRS) is considered FTI and ensure that agencies, bodies, and commissions are maintaining appropriate safeguards to protect the information confidentiality. [IRS 1075] Tax return information that is not provided by the IRS falls under PII.
Full Live Test	Exercise plan incorporates real scenarios and injects into the exercise.
General Support System (GSS)	An interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people.
Health Insurance Portability and Accountability Act of 1996	An act that amended the Internal Revenue Code of 1986, to improve portability and continuity of health insurance coverage in the group and individual markets; to combat waste, fraud, and abuse in health insurance and health care delivery; to promote the use of medical savings accounts; to improve access to long-term care services and coverage; to simplify the administration of health insurance; and for other purposes.
HHS Computer Security Incident Response Center	A capability set up for assisting in responding to computer security-related incidents; also called a Computer Incident Response Team (CIRT) or a CIRC (Computer Incident Response Center, Computer Incident Response Capability).
HHS Privacy Incident Response Team	The FISMA system IRT may consist of federal employees or contractors and must fulfill all of the FISMA system-level responsibilities identified in the HHS IS2P Appendix A Section 13, OpDiv CSIRT, and applicable responsibilities under the HHS IS2P Appendix A Section 14, HHS PIRT. The FISMA system IRT reports to the CMS CCIC IMT, which is responsible for CMS-wide incident management.
Hotwash	A debrief conducted immediately after an exercise or test with the staff and participants.

Terms	Definitions
Hybrid Test	An exercise with some live scenarios facilitated by a response team for realism (probes, scans, email spoofing, etc.);
Incident	A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices
Incident Management Team	CMS IMT provides 24X7 incident management support for the enterprise. It is a single communication point for CMS leadership for security incidents and updates.
Incident Response	Incident response outlines steps for reporting incidents and lists actions to resolve information systems security and privacy related incidents. Handling an incident entails forming a team with the necessary technical capabilities to resolve an incident, engaging the appropriate personnel to aid in the resolution and reporting of such incidents to the proper authorities as required, and report closeout after an incident has been resolved.
Individual Health Information	Individually Identifiable Health Information is a subset of health information including demographic data collected concerning an individual that: • Is created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse • Relates to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual or the past, present, or future payment for the provision of healthcare to an individual, and meets either of the following: • Identifies the individual • There is a reasonable basis to believe the information can be used to identify the individual
Information System Security Officer	Person responsible for ensuring the security of an information system throughout its life cycle, from design through disposal. Synonymous with System Security Officer (SSO). Individual assigned responsibility by the Senior Agency Information Security Officer, authorizing official, management official, or Information System Owner for maintaining the appropriate operational security posture for an information system or program.
Information Systems Security and Privacy Policy	This Policy provides direction to all CMS employees, contractors, and any individual who receives authorization to access CMS information technology (IT) systems or systems maintained on behalf of CMS to assure the confidentiality, integrity, and availability of CMS information and systems. As the federal agency responsible for administering the Medicare, Medicaid, Children's Health Insurance Program (CHIP), and Health Insurance Marketplace (HIM); CMS collects, creates, uses, discloses, maintains, and stores personal, healthcare, and other sensitive information subject to federal law, regulation, and guidance.

Terms	Definitions
Information Technology	The term information technology with respect to an executive agency means any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. This includes equipment used by the executive agency directly or is used by a contractor, under a contract with the executive agency; or use of that equipment, to a significant extent, in the performance of a service or the furnishing of a product; includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance). This includes peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources; but does not include any equipment acquired by a federal contractor incidental to a federal contract. Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. In the preceding sentence, equipment is used by an executive agency if, the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.
Injects	Injects are scenario based exercises created by a functional exercise team during one of several phases (e.g., Development Phase, Conduct Phase for testing, training and exercise programs for IT plans and capabilities). An example inject is, A Controller would play the role of the Chief Information Officer and would call the Team Chief to provide information and request follow-on action. Expected actions by the Team chief or other exercise participants are documented, to aid controllers, simulators, or data collectors in anticipating what actions will result from the inject. For more information on injects see: NIST SP 800-84, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities (page B-8 at: http://csrc.nist.gov/publications/nistpubs/800-84/SP800-84.pdf
Insider Attack	Insider attacks can provide the greatest risk. In an insider attack, a trusted user or operator attempts to damage the system or compromise the information it contains
Insider Threat	An insider threat generally defined as a current or former employee, contractor, or other business partner who has or had authorized

Terms	Definitions
	access to an organization's network (system or data). Intentionally misused that access to negatively affect the confidentiality, integrity, or availability of the organization's information or information systems.1 Insider threats, to include sabotage, theft, espionage, fraud, and competitive advantage are often carried out through abusing access rights, theft of materials, and mishandling physical devices. Insiders do not always act alone and may not be aware as Insiders, facilitate aiding a threat actor (i.e., the unintentional insider threat). It is vital that organizations understand normal employee baseline behaviors and ensure employees understand how being used as conduit information can be obtained.
Intrusions or Break-Ins	An intrusion or break-in is entry into and use of a system by an unauthorized individual.
Malicious Code	Malicious code is software or firmware intentionally inserted into an information system for an unauthorized purpose.
Malicious Software (Malware)	Malicious code is software based attacks used by crackers/hackers to gain privileges, capture passwords, and/or modify audit logs to exclude unauthorized activity. Malicious code is particularly troublesome because to masquerade its presence and, thus, is often difficult to detect. Self-replicating malicious code such as viruses and worms can replicate rapidly, thereby making containment an especially difficult problem. The following is a brief listing of various software attacks: 1. **Virus:** It is propagated via a triggering mechanism (e.g., event time) with a mission (e.g., delete files, corrupt data, send data). 2. **Worm:** An unwanted, self-replicating autonomous process (or set of processes) that penetrates computers using automated hacking techniques. 3. **Trojan Horse:** A useful and innocent program containing additional hidden code that allows unauthorized computer network exploitation (CNE), falsification, or destruction of data. 4. **Spyware:** Surreptitiously installed malicious software intended to track and report the usage of a target system or collect other data the author wishes to obtain. 5. **Rootkit Software:** Software intended to take full or partial control of a system at the lowest levels. Contamination defined as inappropriate introduction of data into a system. 6. **Privileged User Misuse:** Privileged user misuse occurs when a trusted user or operator attempts to damage the system or compromise the information it contains. 7. **Security Support Structure Configuration Modification:** Software, hardware and system configurations contributing to the Security Support Structure (SSS) are controlled, being an essential to maintaining the security policies of the system

Terms	Definitions
	Unauthorized modifications to these configurations can increase the risk to the system.
Major Application (MA)	An application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.
Master Scenario Events List (MSEL)	A chronologically sequence outline of the simulated events and key event descriptions that participants will be asked to respond to during an exercise.
Message Inject	A pre-scripted message will be given to participants during the course of an exercise.
Office of Management and Budget	The Office of Management and Budget (OMB) designated the Department of Homeland Security (DHS) and the National Institute of Standards and Technology (NIST) as authorities to provide guidance to federal agencies for implementing information security and privacy laws and regulations, including FISMA, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and the Privacy Act of 1974 ("Privacy Act"). The Privacy Act addresses CMS applicable information security and privacy requirements, arising from federal legislation, mandates, directives, executive orders. The Department of Health and Human Services (HHS) policy by integrating NIST SP-800-53v4, Security and Privacy Controls for Federal Information Systems and Organizations, with the Department of Health and Human Services Information Systems Security and Privacy Policy (IS2P) and specific programmatic legislation and CMS regulations. Appendix B lists these authoritative references.
Paper Inject/Event	A specific activity executed as part of a Master Scenarios Event List (MSEL), MSEL is a collection of pre-scripted events intended to guide an exercise towards specific outcomes. Paper injects drive exercise play. The exercise planning process determines the participants, exercise scenario, injects and the execution order of the course of the exercise. Planners must tailor injects for each exercise to meet the desired outcomes. For example, if the exercise centers on assessing the ability to detect and properly react to hostile activity, the exercise planners would need to structure one or more scenarios that involve hostile activities against the target IT assets. The exercise planner would design these scenarios to stimulate the training audience and elicit responses that that match the desired outcomes of the specific exercise and the overarching objectives.
Participant Guide	An exercise document that typically contains the exercise's purpose, scope, objectives, and scenario, and a copy of the IT plan being exercised.

Terms	Definitions
Planner(s)	• The group responsible for planning and executing the exercise in a realistic manager.
Privacy Incident	A Privacy Incident is a Security Incident that involves Personally Identifiable Information (PII) or Protected Health Information (PHI), or Federal Tax Information (FTI) where there is a loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users or any other than authorized purposes. Users must have access or potential access to PII, PHI, and/or FTI in usable form whether physical or electronic. Privacy incident scenarios include, but are not limited to: • Loss of federal, contractor, or personal electronic devices that store PII, PHI and/or FTI affiliated with CMS activities (i.e., laptops, cell phones that can store data, disks, thumb-drives, flash drives, compact disks, etc.) • Loss of hard copy documents containing PII, PHI and/or FTI • Sharing paper or electronic documents containing PII, PHI and/or FTI with individuals who are not authorized to access it • Accessing paper or electronic documents containing PII, PHI and/or FTI without authorization or for reasons not related to job performance • Emailing or faxing documents containing PII, PHI and/or FTI to inappropriate recipients, whether intentionally or unintentionally • Posting PII, PHI and/or FTI, whether intentionally or unintentionally, to a public website • Mailing hard copy documents containing PII, PHI and/or FTI to the incorrect address Leaving documents containing PII, PHI and/or FTI exposed in an area where individuals without approved access could read, copy, or move for future use
Protected Health Information	Individually identifiable health information that is: • Transmitted by electronic media, • Maintained in electronic media, or • Transmitted or maintained in any other form or medium. Note: PHI excludes individually identifiable health information in employment records held by a covered HIPAA entity in its role as employer.
Personal Identifiable Information	Any information about an individual including, but not limited to: education, financial transactions, medical history, and criminal or employment history; and information which can be used to distinguish or trace an individual's identity, such as the name, social security number, date and place of birth, mother's maiden name, biometric

Terms	Definitions
	records, etc., including any other personal information, which is linked or linkable to an individual. Information which can be used to distinguish or trace an individual's identity, such as the name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.
Pre-Breach Analysis Team	The CMS Pre-BAT, managed by the CMS Information Security and Privacy Group, with the assistance from the CMS Business Owner/Information Systems Owner (ISOs) and SOP staff as necessary, reviews, triages privacy incidents, and refers to the CMS BAT for a formal risk assessment when needed.
Privileged User Misuse	Privileged user misuse occurs when a trusted user or operator attempts to damage the system or compromise the information it contains.
Red Team	A group of people authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an enterprise's security posture. The Red Team's objective is to improve enterprise Information Assurance by demonstrating the impacts of successful attacks and by demonstrating what works for the defenders (i.e., the Blue Team) in an operational environment.
Risk	The likelihood that a threat will exploit a vulnerability. For system may not have a backup power source; hence, it is vulnerable to a threat, such as thunderstorm, which creates a risk.
Risk Executive (Function)	An individual or group within an organization that helps to ensure that: (i) security risk-related considerations for individual information systems, to include the authorization decisions for those systems, are viewed from an organization-wide perspective with regard to the overall strategic goals and objectives of the organization in carrying out its missions and business functions; and (ii) managing risk from individual information systems is consistent across the organization, reflects organizational risk tolerance, and is considered along with other organizational risks affecting mission/business success.
Risk Management Handbook	The Risk Management Handbook (RMH) compiles CMS standards, requirements, directives, practices, and procedures for protecting CMS information and information systems.
RiskVision	Incident report and tracking system used by HHS and CMS.
Rootkit Software	A type of malicious software (Malware) - Software intended to take full or partial control of a system at the lowest levels. Contamination defined as inappropriate introduction of data into a system.
RSA Archer	RSA Archer is a modulated platform that assists in building an efficient, collaborative governance, risk and compliance (GRC)

Terms	Definitions
	program. For more details see: http://www.ndm.net/rsa/Archer-GRC/archer-grc-modules
Rules of Behavior	Guidelines describing permitted actions by users and the responsibilities when utilizing a computer system. The rules that have been established and implemented concerning use of, security in and acceptable level of risk for the system. Rules will clearly delineate responsibilities and expected behavior of all individuals with access to the system. Rules should cover such matters as work at home, dial-in access, connection to the Internet, use of copyrighted works, unofficial use of federal government equipment, the assignment, and limitation of system privileges, and individual accountability.
Scenario	• A sequential, narrative account of a hypothetical incident that provides the catalyst for the exercise and is intended to introduce situations that will inspire responses and thus allow demonstration of the exercise objectives.
Security Incident	In accordance with *NIST SP 800-61 Revision 2, Computer Security Incident Handling Guide*, a security incident is defined as an event that meets one or more of the following criteria: • The successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in any information system processing information on behalf of CMS. It also means the loss of data through theft or device misplacement, loss or misplacement of hardcopy documents and misrouting of mail, all of which may have the potential to put CMS data at risk of unauthorized access, use, disclosure, modification, or destruction • An occurrence that jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices
Security Support Structure Configuration Modification	A type of malicious software (Malware) - Software, hardware and system configurations contributing to the Security Support Structure (SSS) are controlled. SSS is essential to maintaining the security policies of the system, unauthorized modifications to these configurations can increase the risk to the system.
Senior Official for Privacy	The SOP must be an agency official (federal government employee) and must fulfill all of the responsibilities identified in the HHS IS2P Appendix A Section 15, OpDiv SOP. The SOP carries out the CIO's privacy responsibilities under federal requirements in conjunction with the CISO.

Terms	Definitions
Spillage	Instances where sensitive information (e.g. classified information, export-controlled information) is inadvertently place on information systems not authorized to process such information.
Spyware	A type of malicious software (Malware) that's surreptitiously installed and intended to track and report the usage of a target system, or collect other data the author wishes to obtain.
Tabletop Exercise	A discussion-based exercise where personnel with roles and responsibilities in a particular IT plan meet in a classroom setting or in breakout groups to validate the content of the plan by discussing the roles during an emergency and the responses to particular emergency. A facilitator initiates the discussion by presenting a scenario and asking questions based on the scenario.
Tabletop Test	An exercise with injects scripted by exercise planners and delivered via paper (cards/discussion).
Technical Vulnerability	A technical vulnerability is a hardware, firmware, or software weakness or design deficiency that leaves a system open to potential exploitation, either externally or internally, thus increasing the risk of compromise, alteration of information, or denial of service.
Test	An evaluation tool that uses quantifiable metrics to validate the operability of a system or system component in an operational environmental specified in an IT plan.
Test Plan	A document that outlines the specific steps performed for a particular test, including the required logistical items and expected outcome or response for each step.
Test, Training, and Exercise (TT&E) Event	An event used to support the maintenance of an IT plan by allowing organizations to identify problems related to an IT plan and implement solutions before an adverse situation occurs.
Test, Training, and Exercise (TT&E) Plan	A plan that outlines the steps taken to ensure that personnel are trained in IT plan roles and responsibilities. TT&E plans exercised to validate the viability of how IT components or systems are tested and to validate the operability in the context of an IT plan.
Test, Training, and Exercise (TT&E) Policy	A policy that outlines an organization's internal and external requirements associated with training personnel, exercising IT plans, and testing IT components.
Test, Training, and Exercise (TT&E) Program	A means for ensuring that personnel are trained in IT plan roles and responsibilities; TT&E plans are exercised to validate the viability; and how IT components or systems are tested to validate operability.
Test, Training, and Exercise (TT&E) Program Coordinator	• A person who is responsible for developing a TT&E plan and coordinating TT&E events.

Terms	Definitions
Threat(s)	The potential to cause unauthorized disclosure, changes, or destruction to an asset. • **Impact:** potential breach in confidentiality, integrity, failure and unavailability of information **Types:** natural, environmental, and man-made
Training	Informing personnel of roles and responsibilities within a particular IT plan and teaching personnel skills related to those roles and responsibilities.
Trojan Horse	A type of malicious software (Malware) – a useful and innocent program containing additional hidden code that allows unauthorized computer network exploitation (CNE), falsification, or destruction of data.
Virus	A type of malicious software (Malware) that is propagated via a triggering mechanism (e.g., event time) with a mission (e.g., delete files, corrupt data, send data).
Vulnerabilities	Any flaw or weakness that can be exploited and may result in a breach or a violation of a system's security policy.
Worm	A type of malicious software (Malware) that is an unwanted, self-replicating autonomous process (or set of processes that penetrates computers using automated hacking techniques.

Appendix C. Applicable Laws and Guidance

Appendix C provides references to both authoritative and guidance documentation supporting the "document." Subsections are organize to "level of authority" (e.g., Statutes take precedence over Federal Directives and Policies). The number on each reference represents a mapping that uniquely identifies the reference within the main body of the document. The brackets [#] in the Roles and Responsibilities section are the actual brackets in the "Policy." In this document, the brackets serve as an example of how the brackets will appear in both sections of the document.

C.1 Statutes

Federal Information Security Modernization Act (FISMA) of 2014
https://www.congress.gov/bill/113th-congress/senate-bill/2521

Health Insurance Portability and Accountability Act of 1996 (HIPAA)
http://www.hhs.gov/hipaa/

The Privacy Act of 1974, as amended (5 U.S.C. 552a)
http://www.cms.gov/Research-Statistics-Data-and-Systems/Computer-Data-and-Systems/Privacy/PrivacyActof1974.html

E-Government Act of 2002 (Pub. L. No. 107-347) § 208
https://www.gpo.gov/fdsys/pkg/PLAW-107publ347/content-detail.html

C.2 Federal Directives and Policies

FedRAMP Rev. 4 Baseline
https://www.fedramp.gov/files/2015/03/FedRAMP-Control-Quick-Guide-Rev4-FINAL-01052015.pdf

C.3 OMB Policy and Memoranda

OMB Circular A-130 Management of Federal Information Resources
https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf

OMB M-03-22, Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002
http://www.whitehouse.gov/omb/memoranda_m03-22/

OMB M-16-03, Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements

https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-03.pdf

OMB M-16-04, Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government
https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-04.pdf

OMB M-17-09, Management of Federal High Value Assets
https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-09.pdf

OMB M-14-04, Fiscal Year 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management
https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2014/m-14-04.pdf

OMB M-02-01, Guidance for Preparing and Submitting Security Plans of Actions and Milestones
https://georgewbush-whitehouse.archives.gov/omb/memoranda/m02-01.html

C.4 NIST Guidance and Federal Information Processing Standards

FIPS-199, Standards for Security Categorization of Federal Information and Information Systems
http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

NIST SP 800-18, Guide for Developing Security Plans for Federal Information Systems.
http://dx.doi.org/10.6028/NIST.SP.800-18r1

NIST SP 800-30, Guide for Conducting Risk Assessments
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

NIST SP 800-53-r4, Security and Privacy Controls for Federal Information Systems and Organizations
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

NIST SP 800 53Ar4, Guide for Assessing the Security Controls in Federal Information Systems
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf

NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information

http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf

C.5 HHS Policy

HHS-OCIO-2013-0004 HHS Policy for Personal Use of Information Technology Resources

http://www.hhs.gov/ocio/policy/pol-pers-use-it-resources.html (Intranet Only)

HHS-OCIO-2014-0001 HHS Information System Security and Privacy Policy (HHS IS2P)

HHS Information Security and Privacy Policy (IS2P) – 2014 Edition. To obtain a copy of this document, please email fisma@hhs.gov

HHS- OCIO 2013-0003S HHS Rules of Behavior for Use of HHS Information Resources

http://www.hhs.gov/ocio/policy/hhs-rob.html (Intranet Only)

HHS The Office of the Assistant Secretary for Financial Resources (ASFR)

http://www.hhs.gov/about/agencies/asfr/ (Intranet Only)

C.6 CMS Policy and Directives

CMS Information Systems Security and Privacy Policy (IS2P2)

https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/IS2P2.pdf

C.7 Associated CMS Resources

CMS Risk Management Handbook Chapter 5: Configuration Management

https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html

CMS Risk Management Handbook Chapter 4: Security Assessment and Authorization

https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html

CMS Technical Reference Architecture – Volume 1 – Foundation

2017 Release 1 – Version 1.0, October 11, 2017

https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/CIO-Directives-and-Policies/CIO-IT-Policy-Library-Items/TRA-Volume-I-%E2%80%93-Foundation.html?DLPage=3&DLEntries=10&DLSort=0&DLSortDir=ascending

CMS Technical Reference Architecture – Volume 2 – Network Services

2017 Release 1 – Version 1.0, October 11, 2017

https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/CIO-Directives-and-Policies/CIO-IT-Policy-Library-Items/TRA-Volume-II-%E2%80%93-Network-Services.html?DLPage=3&DLEntries=10&DLSort=0&DLSortDir=ascending

CMS Technical Reference Architecture – Volume 3 – Infrastructure Services

2017 Release 1 – Version 1.0, October 11, 2017

https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/CIO-Directives-and-Policies/CIO-IT-Policy-Library-Items/TRA-Volume-III-Infrastructure-Services.html?DLPage=3&DLEntries=10&DLSort=0&DLSortDir=ascending

CMS Technical Reference Architecture – Volume 4 – Development and Application Services

2017 Release 1 – Version 1.0, October 11, 2017

https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/CIO-Directives-and-Policies/CIO-IT-Policy-Library-Items/TRA-Volume-IV-Development-and-Application-Services.html?DLPage=3&DLEntries=10&DLSort=0&DLSortDir=ascending

CMS Technical Reference Architecture – Volume 5 – Data Management

2017 Release 1 – Version 1.0, October 11, 2017

https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/CIO-Directives-and-Policies/CIO-IT-Policy-Library-Items/TRA-Volume-V-Data-Management.html?DLPage=3&DLEntries=10&DLSort=0&DLSortDir=ascending

ISRA Procedure, March 19, 2009, v1.0 and the supporting ISRA template, v4.0, 3/14/16

Process for determining e-authentication levels for CMS Systems", RMH, VIII, Standard 3.1

Appendix D. Information System Risk Assessment (ISRA) Template

The RMH Chapter 14 Risk Assessment Appendix D – CMS Information System Risk Assessment Template is available on the CMS Information Security and Privacy Library located at:

https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html

Appendix E. CMS Information Security Policy/Standard Risk Acceptance Template

The RMH Chapter 14 Risk Assessment Appendix E – CMS Information Security Policy/Standard Risk Acceptance Template is available on the CMS Information Security and Privacy Library located at:

https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html

Appendix F: Feedback and Questions

Information security and privacy are dynamic fields and as such policies, standards, and procedures must be continually refined and updated. Feedback from the user community is invaluable and ensures that high quality documents are produced and that those documents add value to the CMS community. Should you have any recommendations for improvements to this document, please email the ISPG Policy mailbox at ISPG_Policy_Mailbox@cms.hhs.gov. Your feedback will be evaluated for incorporation into future releases of the document. Questions about any of the material include within this document may also be sent to the ISPG Policy mailbox mailbox.

Appendix G. Plan of Action and Milestones (POA&M) Guide

The RMH Chapter 14 Risk Assessment Appendix G – Plan of Action and Milestones (POA&M) Guide is available under "CFACTS Documents" on the CMS FISMA Controls Tracking System (CFACTS) website located at:

https://cfacts3.cms.cmsnet/apps/ArcherApp/Home.aspx