IT Security Procedural Guide: Risk Management Strategy (RMS) CIO-IT Security-18-91

Revision 3

June 25, 2020

Office of the Chief Information Security Officer

VERSION HISTORY/CHANGE RECORD

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
		Initial Release – March 27, 2019		
N/A	Desai	New Document		N/A
		Revision 1 – May 5, 2017		
1	Feliksa/Dean /Klemens	Updated format and structure, align with current policies and procedures.	Reformatted document to align with current style and structure. Updated to align with current CIO 2100.1 and CIO IT Security 06-30.	Throughout
		Revision 2 – March 14, 2018		
1	Feliksa/Dean /Klemens	Updated to integrate NIST Cybersecurity Framework and scope to IT/Cybersecurity.	Integrate NIST Cybersecurity per Executive Order 13800 and scope to information system and information security.	Throughout
		Revision 3 – June 25, 2020		
1	Dean/ Klemens	Revised to include: • Risk Executive Function • Changed to reflect Enterprise Management Board process • Update references and roles/responsibilities • Included reference to Showstopper Controls • Updated FISMA processes description	Update to current format and style and Federal and GSA guidance.	

Approval

IT Security Procedural Guide: Risk Management Strategy (RMS), CIO-IT Security 18-91, Revision 3, is hereby approved for distribution.

X DocuSigned by:
Bo Berlas
FD7179261615445...

Bo Berlas
GSA Chief Information Security Officer

Contact: GSA Office of the Chief Information Security Officer (OCISO), Policy and Compliance Division (ISP) at ispcompliance@gsa.gov.

Table of Contents

Notes:

- Hyperlinks in running text will be provided if they link to a location within this document (i.e., a different section or an appendix). Hyperlinks will be provided for external sources unless the hyperlink is to a webpage or document listed in Section 1.3. For example, Google Forms, Google Docs, and websites will have links.
- It may be necessary to copy and paste hyperlinks in this document (Right-Click, Select Copy Hyperlink) directly into a web browser rather than using Ctrl-Click to access them within the document.

1 Introduction

Enterprise risk at the General Services Administration (GSA) is handled by the Enterprise Management Board (EMB), chaired by the Deputy Administrator, who is also the Senior Accountable Official for Risk Management (SAORM). For cybersecurity risks, the Chief Information Security Officer (CISO), Authorizing Officials, and subject matter experts facilitate the consistent application of risk management across GSA. The CISO coordinates with the Chief Information Officer (CIO), a member of the EMB, to identify cybersecurity risks for consideration by the EMB. This process satisfies the ERM capability required by Office of Management and Budget (OMB) Memo 16-17, "*OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control*," and the Risk Executive (Function) identified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-39, Revision 1, "*Managing Information Security Risk: Organization, Mission, and Information System View*." The EMB provides an effective agency-wide approach to addressing the full spectrum of GSA's risks by considering the combined array of risks as an interrelated portfolio, rather than addressing risks only within silos.

NIST SP 800-39 describes the integration of the risk management process throughout an organization as occurring at three tiers: (1) organization level; (2) mission/business process level; and (3) information system level. The EMB addresses risk at all three tiers. At the information system level (Tier 3) this is handled by the coordination of the CISO with the CIO to identify cybersecurity risks for EMB consideration.

NIST SP 800-53 includes security control PM-9, Risk Management Strategy, which requires an organization to develop "*a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems*." The GSA OCISO Policy and Compliance Division (ISP) has developed and maintains this document, CIO-IT Security-18-91, to establish a comprehensive approach to managing risk with regard to the operation and use of GSA information systems. GSA follows NIST guidance when assessing and managing information system and security risk.

The primary NIST documents used by GSA in managing risk are:

- NIST SP 800-30, Revision 1, "*Guide for Conducting Risk Assessments*"
- NIST SP 800-37, Revision 2, "*Risk Management Framework For Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*"
- NIST SP 800-39, Revision 1, "*Managing Information Security Risk: Organization, Mission, and Information System View*"
- NIST SP 800-137, "*Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*"
- NIST Cybersecurity Framework, "*Framework for Improving Critical Infrastructure Cybersecurity*"

Executive Order (EO) 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" requires all agencies to use "The Framework for Improving Critical Infrastructure Cybersecurity (the Framework) developed by NIST or any successor document to manage the agency's cybersecurity risk." This NIST document is commonly referred to as the Cybersecurity Framework (CSF).The CSF complements, and does not replace, an organization's risk management process and cybersecurity program. Further information on how the CSF relates to GSA's use of the NIST Risk Management Framework (RMF), including the use of the NIST SP 800-30 risk assessment process in its overall risk management strategy, is provided in Section 5.1.

The listed terms are defined as follows (from the NIST online glossary) when used throughout this guide, unless otherwise stated.

> Cybersecurity - Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.
>
> Information Security Risk - The risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems.
>
> Information System - Related Security Risks - Risks that arise through the loss of confidentiality, integrity, or availability of information or information systems and consider impacts to the organization (including assets, mission, functions, image, or reputation), individuals, other organizations, and the Nation.

1.1 Purpose

This document provides a comprehensive approach for managing risks associated with GSA information systems in accordance with Federal laws, regulations, and requirements; and establishes GSA guidance and processes for all operating units and GSA Services and Staff Offices (S/SO) to follow.

1.2 Scope

This document establishes an integrated, comprehensive approach to identify, measure, and manage risk to GSA operations, assets, and individuals associated with the operation and use of GSA information systems.

1.3 References

Note: GSA updates its Information Technology (IT) security policies and procedural guides on independent cycles which may introduce conflicting guidance until revised documents are

developed. In addition, many of the references listed are updated by external organizations which can lead to inconsistencies with GSA policies and guides. When conflicts or inconsistencies are noticed, please contact ispcompliance@gsa.gov for guidance.

The following references provide guidance, mandates, or direction on managing information system and security risk within GSA.

Federal Laws, Standards and Guidance:

- Department of Homeland Security (DHS) Cybersecurity Directives
- EO 13800, "*Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*"
- Federal Financial Management Improvement Act of 1996 (FFMIA)
- FIPS PUB 199, "*Standards for Security Categorization of Federal Information and Information Systems*"
- NIST Cybersecurity Framework, Version 1.1, "*Framework for Improving Critical Infrastructure Cybersecurity*"
- NIST SP 800-30, Revision 1, "*Guide for Conducting Risk Assessments*"
- NIST SP 800-37, Revision 2, "*Risk Management Framework for Information Systems and Organizations*"
- NIST SP 800-39, "*Managing Information Security Risk*"
- NIST SP 800-53, Revision 4, "*Security and Privacy Controls for Federal Information Systems and Organizations*"
- NIST SP 800-137, "*Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*"
- OMB Circular A-130, "*Managing Information as a Strategic Resource"*
- OMB Memo 16-17, "*OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control*"
- Public Law 113–283, "*Federal Information Security Modernization Act of 2014*''
- Public Law 97-255, "*Federal Managers Financial Integrity Act of 1982 (FMFIA)*"

GSA Directives, Policies, and Procedures:

- GSA Order CIO 2100.1, "*GSA Information Technology (IT) Security Policy*"

The documents below are available on the GSA IT Security Procedural Guides InSite Page.

- CIO-IT Security-01-02, *"Incident Response (IR)"*
- CIO-IT Security-01-05, *"Configuration Management"*
- CIO-IT Security-04-26, *"Federal Information Security Modernization Act (FISMA) Implementation"*
- CIO-IT Security-06-30, "*Managing Enterprise Risk*"
- CIO-IT Security-09-44, "*Plan of Action and Milestones*"
- CIO-IT Security-09-48, "*Security and Privacy Requirements for IT Acquisition Effort*"
- CIO-IT Security-12-64, "*Physical and Environmental Protection"*
- CIO-IT Security-12-66, "*Information Security Continuous Monitoring Strategy*"

- CIO-IT Security-11-51, "*Conducting Penetration Test Exercises*"
- CIO-IT Security-17-80, "*Vulnerability Management Process*"
- CIO-IT Security-18-90, "*Information Security Program Plan"*

GSA IT Security forms are available on the GSA IT Security Forms and Aids InSite Page.

2 Roles and Responsibilities

The complete roles and responsibilities for agency management officials and others with significant IT Security responsibilities are defined fully in Chapter 2 of GSA Order CIO 2100.1. The following sections provide extracted or paraphrased key responsibilities from CIO 2100.1, or other GSA or Federal guidance, regarding managing risks associated with GSA information systems.

2.1 GSA Administrator

Responsibilities include the following:

- Developing and overseeing the implementation of policies, principles, standards, and guidelines on information security; including ensuring timely agency adoption of and compliance with security standards.
- Providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of an agency, and on information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.
- Ensuring that an information security program is developed, documented, and implemented to provide security for all systems, networks, and data that support the operations of the organization.
- Ensuring that information security management processes are integrated with agency strategic and operational, and budgetary processes.
- Ensuring that the CIO, in coordination with the other senior agency officials, reports annually to the GSA Deputy Administrator on the effectiveness of the agency information security program, including the progress of remedial actions.

2.2 Risk Executive (Function)

The Risk Executive (Function) at GSA is handled by the EMB, chaired by the Deputy Administrator who is also the SAORM. For cybersecurity risks, the CISO, Authorizing Officials (AOs), and subject matter experts facilitate the consistent application of risk management across GSA. The CISO coordinates with the CIO, a member of the EMB, to identify cybersecurity risks for consideration by the EMB. As stated in the EMB, the Risk Executive (Function) manages and monitors key organizational risks.

Responsibilities include the following:

- Providing a forum to identify and discuss cross-cutting strategic, reputational, regulatory, operational, cybersecurity, financial and other risks;
- Elevating new or emerging risks and communicating the status of existing risks, including ongoing mitigation efforts;
- Identifying risk owners and considering mitigation strategies and/or corrective actions;
- Maintaining and maturing GSA's risk management framework, including its risk tolerance thresholds, risk appetite, and enterprise risk profile;
- Engaging with other GSA governance groups, as needed, to provide strategic guidance;
- Establishing risk management roles and responsibilities;
- Developing and implementing an organization-wide risk management strategy that guides and informs organizational risk decisions (including how risk is framed, assessed, responded to, and monitored over time;
- Determining organizational risk based on the aggregated risk from the operation and use of information systems and the respective environments of operation; and

2.3 Chief Information Officer (CIO)

Responsibilities include the following:

- Developing and maintaining an agency-wide GSA IT Security Program.
- Establishing reporting requirements within GSA to assess GSA's IT security posture, verifying compliance with Federal requirements and approved policies, and identifying agency-wide IT security needs.
- Reporting annually, in coordination with the other senior agency officials, to the GSA Deputy Administrator on the effectiveness of the agency information security program, including progress of remedial actions.
- Coordinates with the CISO and the Deputy Administrator regarding cybersecurity risks in relation to overall ERM at GSA.

2.4 Chief Financial Officer (CFO)

Responsibilities include the following:

- Ensuring the sufficiency of management and information security controls pertaining to GSA's financial management systems and compliance with Federal Managers' Financial Integrity Act (FMFIA) and Federal Financial Management Improvement Act (FFMIA) requirements.
- Developing and maintaining an integrated agency accounting and financial management system, including financial reporting and internal controls, which comply with FMFIA and FFMIA requirements;
- Ensuring that the appropriate security requirements of CIO 2100.1 are included in all contracts for IT systems designed, developed, implemented, and operated by a contractor that hosts GSA financial systems.

2.5 Senior Agency Official for Privacy (SAOP)

Responsibilities include the following:

- Ensuring GSA information systems that contain Personally Identifiable Information (PII) address any recommendations of the SAOP as part of the system Assessment & Authorization (A&A), including addressing the privacy controls in Appendix J of NIST SP 800-53, Revision 4, as appropriate.
- Developing, implementing, and overseeing personnel security controls for access to PII.

2.6 Chief Information Security Officer (CISO)

Responsibilities include the following:

- Reporting to the GSA CIO on the implementation and maintenance of the GSA's IT Security Program and Security Policies.
- Implementing and overseeing GSA's IT Security Program by developing and publishing security policies and IT security procedural guides that are consistent with CIO 2100.1.
- Assessing risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems supporting the operations and assets of the agency on a periodic basis.
- Testing and evaluating the effectiveness of information security policies, procedures, and practices on a periodic basis.
- Establishing and maintaining a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency.
- Developing and implementing IT security performance measures to evaluate the effectiveness of technical and non-technical safeguards used to protect GSA information and information systems.
- Administering Federal Information Security Modernization Act (FISMA) requirements and coordinating GSA’s annual FISMA security program review and Plan of Action and Milestones (POA&M) implementation.
- Concurring/Non-concurring on ATOs as specified in GSA CIO-IT Security-06-30 and its related A&A procedural guides.
- Coordinates with the CIO and the Deputy Administrator regarding cybersecurity risks in relation to overall ERM at GSA.

2.7 Heads of Services and Staff Offices (HSSOs)

Responsibilities include the following:

- Ensuring adherence and proper implementation of GSA’s IT Security Policy.
- Ensuring that the systems of record under their jurisdiction meet the requirements of the Privacy Act and GSA privacy policies and procedures.

- Ensuring that contractors performing services associated with GSA systems (such as system development, maintenance, or operation) are subject to GSA security requirements.

2.8 Authorizing Official (AO)

Responsibilities include the following:

- Identifying the level of acceptable risk for an IT system or application and determine whether the acceptable level of risk has been obtained.
- Reviewing and approving security safeguards of information systems and issuing ATO approvals for each information system under their jurisdiction based on the acceptability of the security safeguards of the system (risk-management approach).
- Ensuring GSA systems are assessed via operating system and web application scans as defined in CIO-IT Security-17-80. Identified vulnerabilities from the scans shall be resolved and tracked in the systems' POA&Ms in accordance with CIO-IT Security-09-44 and CIO-IT Security-06-30.

2.9 Office of CISO Division Directors

Responsibilities include the following:

- Monitoring adherence and proper implementation of GSA's IT Security Policy and reporting the results to the CISO.
- Reviewing and approving A&A documents to be signed by the appropriate business line representatives and concurred by the CISO or appropriate OCISO personnel.
- Assisting individuals with IT Security responsibilities on security architecture and security engineering principles and practices.

2.10 Information Systems Security Manager (ISSM)

Responsibilities include the following:

- Ensuring adherence and proper implementation of GSA's IT Security Policy.
- Reviewing and coordinating reporting of Security Advisory Alerts (SAA), compliance reviews, security and privacy awareness training, incident reports, contingency plan testing, and other IT security program elements.
- Managing system assessments (including A&A package requirements and Payment Card Industry Data Security Standard [PCI DSS] Report on Compliance [for IT systems that process, store, or transmit payment card data or purchase/credit card numbers]), and forwarding them to the AO and appropriate OCISO Directors

2.11 Information Systems Security Officer (ISSO)

Responsibilities include the following:

- Ensuring the system is operated, used, maintained, and disposed of in accordance with (IAW) documented security policies and procedures. Necessary security controls should be in place and operating as intended.
- Evaluating Security Advisory Alerts (SAAs) issued by the OCISO Security Operations Division and known vulnerabilities to ascertain if additional safeguards are needed, and ensuring systems are patched and securely configured, as appropriate.
- Advising system owners of risks to their systems and obtaining assistance from the ISSM, if necessary, in assessing risk.
- Working with the ISSM and system owners to develop, implement, and manage POA&Ms for assigned systems in accordance with CIO-IT Security-09-44.

2.12 System Owners

Responsibilities include the following:

- Ensuring effective implementation of GSA's IT Security Policy.
- Consulting with the ISSM and ISSO and receiving the approval of the AO, when selecting the mix of controls, technologies, and procedures that best fit the risk profile of the system.
- Participating in activities related to the assessment and authorization of the system to include security planning, risk assessments, security and incident response testing, and contingency planning and testing.
- Ensuring that for each information system, security is planned, documented, and integrated and implemented in accordance with Federal and GSA directives, polices, and guidance.
- Working with the ISSO and ISSM to develop, implement, and manage POA&Ms for assigned systems in accordance with CIO-IT Security-09-44.

2.13 Data Owners

Responsibilities include the following:

- Coordinating with system owners, ISSMs, ISSOs, and Custodians to ensure the data is properly stored, maintained, and protected IAW GSA policies, regulations and any additional guidelines established by GSA.
- Ensuring that data is not processed on a system with security controls that are not commensurate with the sensitivity of the data.

2.14 Contracting Officers (COs) and Contracting Officer's Representative (CORs)

Responsibilities include the following:

- Coordinating with the CISO or other appropriate official as required ensuring that all agency contracts and procurements are compliant with the agency's information security policy and include appropriate security contracting language and security requirements in each contract.

- Ensuring new solicitations for all GSA IT systems includes the security contract language from CIO-IT Security-09-48.

2.15 Custodians

Responsibilities include the following:

- Coordinating with data owners and system owners to ensure the data is properly stored, maintained, and protected.
- Establishing, monitoring, and operating information systems in a manner consistent with GSA policies and standards as relayed by the AO.

2.16 Authorized Users of IT Resources

Responsibilities include the following:

- Complying with all GSA security policies and procedures.
- Reporting any observed or suspected security problems/incidents to the IT Service Desk.

3 GSA OCISO Divisions

The OCISO consists of the CISO and four divisions providing operational, engineering, policy, and security officer support as detailed in the following subsections.

3.1 Security Operations Division

The Security Operations (SecOps) Division (ISO) provides real-time operational security through Security Operating Center (SOC) and enterprise network security capabilities. This division supports IT division offices by providing vulnerability scanning and operational security services at the enterprise level including managing firewalls, intrusion prevention systems, and the Enterprise Logging Platform (ELP).

3.2 Security Engineering Division

The Security Engineering (SecEng) Division (ISE) provides security consulting and engineering support for systems and emerging IT and IT security initiatives. In addition, this division provides incident response and technical benchmarks. ISE directly supports IT division offices in developing technical security standards and architectural security standards in the support of IT systems.

3.3 Policy and Compliance Division

The Policy and Compliance Division (ISP) provides management and maintenance of the GSA Plan of Action & Milestones (POA&M), Continuous Monitoring, and Security Awareness and Role Based Training programs. This division also manages the process to create and maintain GSA IT security policies, the coordination of cybersecurity audits, and the FISMA compliance

reporting process. ISP provides information to the CISO and AOs to monitor the implementation of the GSA IT Security policy.

3.4 ISSO Support Division

The ISSO Support Division (IST) provides ISSO and ISSM support services to all Staff Offices and Services systems. The division facilitates integrating IT security in programs and compliance with required security and privacy requirements. IST services assist the CISO and AOs during the assessment process to grant an Authorization to Operate.

4 GSA Enterprise Management Board (EMB)

GSA's EMB has as one of its focus areas the management of enterprise wide risks. The EMB includes the use of risk profiles that identified and updated at least annually and issues are discussed quarterly as part of the EMB agenda. Cybersecurity risks are included in the EMB's risk profiles. The profiles characterize risk by:

- Describing the risk, including a risk rating and trend;
- Identifying the accountable executive and their Service/Staff Office;
- Listing the GSA strategic objectives affected;
- Providing the potential impacts if the risk is realized;
- Describing the current status and progress made on actions performed;
- Listing planned mitigations and milestones to further mitigate and reduce the risk.

5 GSA Information System and Information Security Risk Management Process

GSA's information and information system security risk strategy is based on assessing and managing risks as part of the following processes.

- The A&A process followed by a GSA (federal or contractor) system to achieve its initial ATO as defined in CIO-IT Security-06-30.
- The vulnerability management process described in CIO-IT Security-17-80.
- The continuous monitoring process described in CIO-IT Security-12-66.
- GSA's Continuous Diagnostics and Mitigation (CDM) implementation in accordance with DHS/OMB guidance.
- The FISMA processes (i.e., annual self-assessments, FISMA metrics analysis) described in CIO-IT Security-04-26.
- Any penetration tests required as defined in CIO-IT Security-06-30, and CIO-IT Security 11-51.
- Audits (e.g., Inspector General [IG], FISMA) performed on GSA's system and security processes.
- Incidents/Events identified by internal or external activities as described in CIO-IT Security-01-02.
- The POA&M process as defined in CIO-IT Security-09-44.

5.1 Aligning NIST Risk Assessments and the CSF

As described in the introduction, GSA adheres to NIST guidance as it relates to risk management. All of GSA's A&A processes have the NIST RMF as a foundation. Risk assessments are performed in accordance with NIST SP 800-30. GSA manages, tracks, and submits FISMA, President's Management Council (PMC), and CSF metrics and performance measures which are aligned to the CSF core functions to inform risk management decisions and planning. As required by EO 13800, GSA has aligned its risk management process with the NIST CSF core functions as described below.

- **Identify (ID):** Develop an organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
    - GSA has identified its high value/critical assets which guides how GSA prioritizes risk resolution.
    - Vulnerabilities are identified and documented, including threats, likelihoods, and impacts, via the multiple processes listed at the beginning of Section 5.
    - The ISE Division receives threat intelligence from multiple sources and communicates this information to GSA's information security community.
    - As part of this document and CIO-IT Security-06-30, risk prioritization and tolerance are identified.
    - Systems categorized as FIPS 199 High or Moderate typically have a lower risk tolerance than systems categorized as FIPS 199 Low systems with publicly available data.
- **Protect (PR):** Develop and implement appropriate safeguards to ensure delivery of critical infrastructure services.
    - GSA's adherence to the NIST RMF process guides how systems are protected by security categorization, security control selection and implementation, and remediation of risks to protect systems.
    - CIO-IT Security 17-80 and CIO-IT Security-12-64 provide processes for managing vulnerabilities to address where additional protection is needed.
- **Detect (DE):** Develop and implement appropriate activities to identify the occurrence of a cybersecurity incident.
    - Vulnerabilities may be detected and documented, including threats, likelihoods, and impacts, via the multiple processes listed at the beginning of Section 5.
    - Incidents and events may detected by GSA's perimeter defenses such as firewalls, Intrusion Detection Systems/Intrusion Prevention Systems (IDS/IPS), or the Enterprise Logging Platform.
    - Users may detect unusual or abnormal items or behavior in systems or applications (e.g., phishing emails) and report them to the IT Helpdesk.
- **Respond (RS):** Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
    - As incidents are responded to in accordance with CIO-IT Security-01-02, risks based on the incidents and vulnerabilities exploited will be shared as appropriate.

    - As part of incident after action/lessons learned reports and semi-annual testing of the incident response plan, the plan and processes within it are updated to improve future response actions.
- **Recover (RC):** Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.
    - Although recovery is generally not a part of assessing risks, lessons learned during recovery from incidents provide feedback that can be used to improve response and recovery processes and reduce risks in the future.

For more information on GSA's alignment of the RMF to the CSF, refer CIO-IT Security-06-30.

5.2 Assessing Information System and Information Security Risk

GSA follows the NIST SP 800-30 risk assessment process when assessing Information system and information security risks. That process consists of the following steps and tasks:

- Prepare for Assessment
- Conduct Assessment
    - Identify Threat Sources and Events
    - Identify Vulnerabilities and Predisposing Conditions
    - Determine Likelihood of Occurrence
    - Determine Magnitude of Impact
    - Determine Risk
- Communicate Results
- Maintain Assessment

Preparing for an assessment will be unique to the various processes listed earlier (e.g., penetration tests, A&A process, audits) and are covered in the GSA IT Security Procedural Guides for those processes and, in general, in CIO-IT Security-06-30 with regard to security assessment planning. For these reasons, preparing for the assessment will not be covered in this document. The following sections address the steps and tasks in conducting risk assessments, communicating results, and maintaining assessments.

5.3 Conducting Risk Assessments

5.3.1 Identifying Threat Sources and Events

The OCISO ISE division identifies the threat landscape for GSA and assists with co-relating the threat scenarios or viable threats with existing vulnerabilities that these threats can take advantage of in the GSA environment. ISE also manages GSA's Threat Awareness Program, as described in CIO-IT Security-01-02. The ISE reviews indicators of compromise (e.g. domains/ IP addresses of known malicious actors, hashes of malicious files, traffic excerpts of suspicious activity, etc.) from threat intelligence for actionable information and shares this information with relevant system owners,

United States-Computer Emergency Readiness Team (US-CERT), and other government agencies as needed. US-CERT coordinates communication of threat intelligence information between GSA and other Federal agencies. ISE implements proactive blocking of IP addresses, Uniform Resource Locators (URLs), hashes, fraudulent email senders, as necessary. Appendix C of CIO-IT Security-01-02 identifies tools and sources GSA OCISO uses for threat information. They include external entities such as US-CERT, FireEye Partners, and GSA enterprise network and security monitoring tools.

On a system-by-system basis, individual threat sources/events (e.g., agents, vectors) are identified in accordance with the threat taxonomy in NIST SP 800-30. Additional threat information may be provided from sources such as CDM tools (attack vectors) and other automated tools.

5.3.2 Identify Vulnerabilities and Predisposing Conditions

Information system and information security vulnerabilities and predisposing conditions may be identified by the processes described below and listed in Section 5, above.

A&A process followed by a GSA system to achieve its initial ATO. Every system at GSA undergoes an A&A process leading to an ATO. Each A&A process described in CIO-IT Security-06-30 requires an assessment be performed. The assessment may reveal vulnerabilities based on any of the following activities. Any findings resulting from these activities must be assessed for risk.

- Completion of GSA's NIST SP 800-53 test cases associated with the NIST controls required by the system's FIPS 199 categorization and A&A process. This task includes the assessment of information security architectures and integration of security into the development process.
- Vulnerability and configuration scans performed as part of the A&A process as documented in CIO-IT Security-06-30.
- Penetration tests completed as part of the system's A&A process requirements as documented in CIO-IT Security-06-30 and CIO-IT Security-11-51.

Vulnerability management process described in CIO-IT Security-17-80. Systems are scanned by various vulnerability scanning tools on a periodic basis as identified in the 06-30 Scanning Parameter Spreadsheet. Verified findings from the scans, as identified in CIO-IT Security-17-80 must be assessed for risk.

Continuous monitoring process described in CIO-IT Security-12-66. Systems in GSA's Ongoing Authorization (OA) Program must adhere to the technical and non-technical assessment of the security controls identified in CIO-IT Security-12-66. Any findings from the automated or manual assessments must be assessed for risk.

GSA's CDM implementation in accordance with DHS/OMB guidance. GSA has implemented CDM tools per DHS/OMB guidance. As the results of the CDM tools are verified and integrated into GSA's vulnerability and ISCM processes, any findings will need to be assessed for risk.

FISMA processes (i.e., annual self-assessments, FISMA metrics analysis) described in CIO-IT Security-04-26. FISMA of 2014 requires annual self-assessments, and DHS/OMB requires agencies to submit quarterly FISMA metrics regarding various aspects of security that are compiled into agency-specific and government-wide risk management assessment (RMA) scorecards. The scorecards are provided to Agencies every quarter. The RMA scorecards are grouped by the FISMA metrics and CSF domains with associated risk ratings (e.g., Managing Risk, At Risk, High Risk, or Not Applicable) for the individual groups and summarized at the group and overall agency level. This data is used to guide the remediation of risks based on OMB/DHS guidance/requirements.

Audits (e.g., IG, FISMA) performed on GSA's system and security processes. Audits (internal and external) are performed regularly on GSA systems and security processes. Any audit findings must be assessed for risk.

Incidents/Events identified by internal or external activities. Incidents may be reported by external or internal entities or events may be discovered through network/system monitoring, user reports, or threat intelligence sources. The incident response, monitoring, or threat intelligence actions may identify findings/conditions that need to be assessed for risk. For example, GSA participates in DHS's Cybersecurity Coordination Assessment, and Response (C-CAR) process and complies with DHS Cybersecurity Directives (i.e., Emergency Directives [EDs], Binding Operational Directives [BODs]). Both C-CAR and EDs/BODs identify events or vulnerabilities and mandate GSA responses to them.

5.3.3 Determine Likelihood of Occurrence

Likelihood is determined manually using data provided by automated tools and system/organizational conditions. As described in NIST SP 800-30, likelihood of an adverse impact is determined by considering:

- How likely it is that threat sources (adversarial or non-adversarial) could cause an event to occur?
- How likely is it, if initiated, that an event would result in an impact?

GSA's scanning and CDM tools provide information that can inform the answers to the questions above. For example, these tools as well as GSA's threat intelligence may indicate if there are known exploits of vulnerabilities, if the known exploits are readily available, and if there has been evidence of the exploits being used elsewhere or targeted at GSA. Additional tools (e.g., a Governance, Risk, and Compliance [GRC] tool) or additional capabilities in existing tools may provide additional automation of likelihood determination in the future.

5.3.4 Determine Magnitude of Impact

The magnitude of impact of a threat event causing harm to the organization's assets, individuals, or organizations or the Nation is also manually determined assisted by data from the same tools described when determining likelihood. Impact is influenced by factors such as

resiliency, spread or containment of the event, the assets susceptible to an event, and weighting factors such as if an asset is a High Value Asset (HVA) listed in GSA's HVA inventory.

5.3.5 Determine Risk

Risk is determined by both automated and manual methods. Per NIST SP 800-30, risk consists of combining the likelihood of a threat event occurring with the level of impact it would cause. Similar to likelihood, GSA automated tools used as part of its vulnerability management process, CDM implementation, and penetration testing generally provide a risk or vulnerability score based on the results of findings. The DHS risk scoring methodology, Agency-Wide Adaptive Risk Enumeration (AWARE), is used within the CDM tool implementation to provide automation assistance for prioritizing the mitigation of vulnerabilities and risks identified by CDM tools. Manual assessments (e.g., test cases, manual part of penetration tests) will have risk determined manually. A more detailed description of how information system risks are assessed is provided in CIO-IT Security-06-30.

Note: A tool's risk rating is not necessarily the final risk rating for a vulnerability and its possible exploitation. Other factors, such as the environment where the vulnerability exists, automated or manual safeguards that provide additional protection, etc. may cause assessors to raise or lower the risk of a threat event causing an adverse impact.

DHS/OMB compiles FISMA Risk Management Assessment (RMA) scorecards as part of annual FISMA analysis and reporting. The RMA scorecards are grouped by the FISMA metrics and Cybersecurity Framework domains with associated risk ratings (e.g., Managing Risk, At Risk, High Risk, or Not Applicable) for the individual groups and summarized at the group and overall GSA level. GSA considers the RMA scorecard and its underlying data as part of its risk remediation and mitigation process.

5.4 Communicating Results

5.4.1 Communicating Risk Assessment Results

The results of risk assessments are communicated using multiple methods. The primary means used are:

- **Security Assessment Reports (SAR).** SARs are prepared as part of a system's A&A process and include all risks determined as part of the assessment. Certain A&A processes (defined in CIO-IT Security-06-30) will not have a formal SAR, but they will still assess risk as part of an assessment of the system.
- **Penetration Test Reports (when required).** Systems with a SAR will include the results of penetration tests in the overall SAR for a system. For systems without a formal SAR a separate penetration test report will be prepared.
- **Dashboards.** GSA's automated tools (CDM and vulnerability scanning) include dashboards or similar features where authorized personnel can review risk results from the automated tool assessments.

- **Plan of Action and Milestones (POA&M).** POA&Ms are required for every system at GSA. Subsystems, as defined in CIO-IT Security-06-30, typically have their POA&Ms included in the FISMA system they reside on. In special situations, after coordination with the OCISO, they may have their own POA&M. GSA's POA&M process is described in CIO-IT Security-09-44 and includes reports on the effectiveness of POA&Ms in managing and mitigating risks. Reports are provided to personnel responsible for the security of individual systems, with summary reports provided to GSA ISSMs, IS Directors, and the CISO.

5.4.2 Sharing Risk-Related Information

Sharing of risk-related information within GSA (but outside of IS) is at the determination of the CISO in collaboration with AOs, ISSMs, IS Directors, and subject matter experts within the OCISO. Part of the collaboration described is to determine which risks are appropriate to become a part the overall GSA EMB process and be entered into the GSA Cyber Risk Profile.

The CISO, in consultation with the IS Directors and GSA Executive Management, make the determination on what risk information should be shared externally. The separate CDM and FISMA reporting processes require certain risk related information be shared with DHS and OMB by law and Federal regulation. Any risks arising from the CDM and FISMA reporting processes (e.g. FISMA IG audits, RMA reports) are communicated with the GSA Administrator and Deputy Administrator by the GSA CIO and CISO.

5.5 Maintaining Assessments

5.5.1 Monitoring Risk Factors

Risk factors, such as threat sources, vulnerabilities, etc., are monitored by the assessment processes described earlier. The ISE and ISO Divisions update threat information as part of the Threat Awareness Program described in CIO-IT Security 01-02. Vulnerabilities are monitored via all of the assessment processes described, some of those processes occur as often as weekly, others annually, and others as an A&A or security assessment process requires.

5.5.2 Updating Risk Assessments

Similar to monitoring of risk factors, updating of risk assessments occurs dependent upon the security process being followed. POA&Ms are expected to be maintained regularly as new vulnerabilities/risks are identified, as actions within the POA&M are performed. POA&Ms are required to be updated at least quarterly. Automated tools (CDM, vulnerability scanners) will update as the tools execute and identify either new vulnerabilities/risks or that previous vulnerabilities/risks have been resolved. The vulnerabilities the automated tools check for are updated on a regular basis by the tool vendors, details are in CIO-IT Security-17-80.

6 Managing Information System and Security Risk

6.1 Risk Tolerance

GSA's informal risk tolerance strategy is based on:

- System categorizations according to FIPS 199 levels;
- System A&A process followed;
- CISO mandated Showstopper capabilities/associated controls as defined in CIO-IT Security-06-30;
- DHS Cybersecurity directives;
- Type of data (PII, other sensitive data, publicly available data);
- Accessibility of the system (Internet facing or internal access only).

Systems categorized as FIPS 199 High or Moderate typically have a lower risk tolerance than systems categorized as FIPS 199 Low systems with publicly available data. Similarly, systems with PII or other sensitive data have a lower risk tolerance than systems without such data. Systems accessible from the Internet also have a lower risk tolerance, especially if they can be used as an avenue to internal systems. The GSA A&A process a system follows to receive an ATO is, in part, determined by the risks of the system and its data being exploited, which in turn impacts the determination of risk tolerance for the system. For example, a system following the CIO-IT Security-14-68, "*Lightweight Security Authorization Process,"* will have a higher risk tolerance due to the restrictions on the types of systems that can use that process compared to a system following the standard A&A process. CISO Showstopper capabilities/controls that are not fully satisfied may lead to a system not being authorized due to the risk involved and, at a minimum, must have an Acceptance of Risk letter approved with a plan on how the risk can be mitigated or resolved. GSA's risk tolerance is summarized by the following statements.

- Risk mitigation will be the appropriate risk response for all Very High/Critical and High risk vulnerabilities that can be exploited from the Internet which cannot be accepted, avoided, shared, or transferred.
- Risks from vulnerability scans must be addressed in the following manner:
    - For Internet-accessible IP addresses
        1. Any Critical (Very High) scan vulnerabilities must be remediated within 15 days.
        2. Any High scan vulnerabilities must be remediated within 30 days.
        3. Any Moderate scan vulnerabilities must be remediated within 90 days.
    - For all other assets
        1. Any Critical (Very High) and High scan vulnerabilities must be remediated within 30 days.
        2. Any Moderate scan vulnerabilities must be remediated within 90 days.
    - Low/Very Low risk vulnerabilities will be addressed on a case-by-case basis as specified in CIO-IT Security-06-30.

6.2 Risk Responses

GSA responds to identified risks is described in the following sections.

6.2.1 Risk Acceptance

Risk acceptance will be used when the appropriate risk is deemed to be Moderate or Low/Very Low depending on particular situations or conditions. The AO may accept the risk for GSA systems that have undergone the ATO process and are granted an ATO with conditions until all of their respective system's findings are remediated in the prescribed time as determined in the conditions of their authority to operate the system.

Risk acceptance may also be an acceptable response for Very High/Critical and High vulnerabilities that cannot be exploited from the Internet on a mission critical system that cannot be patched. Risk acceptance may also be requested from GSA AOs for systems meeting one of the following conditions:

- Have budgetary constraints that limit remediation efforts;
- Legacy systems that cannot be patched;
- Systems that are scheduled for disposal.

CIO-IT Security-06-30 establishes Acceptance of Risk (AoR) letters as the means to document accepted risks higher than Very Low/Low risks. An AO may approve Moderate risks via an AoR letter; AoR letters for Very High/Critical and High risks must be approved by the AO and concurred by the CISO. Very Low/Low risks will be addressed on a case-by-case basis.

6.2.2 Risk Avoidance

Risk avoidance will be used when the appropriate risk is deemed to exceed the organizational risk tolerance. If risk avoidance is used for any particular risk, specific actions must take place to eliminate the activities or technologies that are the basis for the risk.

GSA will use risk avoidance for all technologies that have Very High/Critical or High vulnerabilities that can be exploited from the Internet but cannot be mitigated. Any system meeting this criteria may be presented to GSA's CISO with a recommendation to shut down or shut off the system from the Internet. The recommendation must also describe the mission and business impact of these actions.

6.2.3 Risk Mitigation

Risk mitigation will be the appropriate risk response for all Very High/Critical and High risk vulnerabilities that can be exploited from the Internet and cannot be accepted, avoided, shared, or transferred. Risk mitigation measures will be employed based on prioritization. In general, the prioritization aligns with the level of risk (i.e., Very High/Critical risks should be addressed prior to High risks); however, when there are multiple risks at the same level, system and security personnel coordinate to establish which risks will be addressed first. Prioritization is typically a manual process including criteria such as the probability of vulnerability

exploitation, material business impact if vulnerability is successfully exploited, compliance requirements, evaluation of attack vectors and exposures, level of assets (i.e., High Value and Critical assets prioritized above others), and the cost and business impact of remediation activities and controls. The DHS AWARE process will assist in automating prioritization for risks identified as part of the CDM program.

6.2.4 Risk Sharing or Transfer

GSA will use risk sharing or risk transfer when GSA is responsible for one piece of the hardware or software stack and another agency or vendor is responsible for another piece of the hardware or software stack. Contractor Owned/Contractor Operated (COCO) and cloud-based systems may meet these criteria. All GSA resources that fit these criteria must have their associated risks fully documented in a formal Interconnection Security Agreement (ISA).

6.2.5 Response to Change

GSA monitors changes to its information systems and their architectures by periodically assessing risks at the mission/business process levels in which those systems operate.

- **Information System:** Changes that occur in GSA information systems (including hardware, software, and firmware) that can introduce new risk or change existing risk. GSA has established a rigorous configuration change management process. Any IT changes are requested through a defined CM approval process (e.g., a chartered Change Control Board [CCB]) using automated or manual processes to document the nature of changes, their criticality, impacts on the user community, testing and rollback procedures, stakeholders, and points of contact. System changes are tested and validated prior to implementation into the production environment. Configuration settings and configuration baselines are updated as necessary to meet new technical and/or security requirements and are controlled through the CM process. The CM process requires testing/validating changes where the scope of the change has a major impact on agency reputation, has a large scope or has the potential for significant monetary impact. Additional details on change management can be found in CIO-IT Security-01-05.
- **Environments of Operation:** Environmental and operational considerations include, but are not limited to, missions/business functions, threats, vulnerabilities, mission/business processes, facilities, policies, legislation, and technologies.

6.3 Risk Management Strategy Effectiveness

The effectiveness of GSA's risk management will be determined by evaluating how effective implemented risk response measures, including the implementation of any remediation or compensating controls, have been in reducing identified risk to the desired level. GSA monitors the effectiveness of its risk management framework initially before a system goes into production and through analyzing the results of the following processes.

- Vulnerability management process described in CIO-IT Security-17-80.
- Continuous monitoring process described in CIO-IT Security-12-66 (for systems in the OA program).
- GSA's Continuous Diagnostics and Mitigation (CDM) implementation in accordance with DHS/OMB guidance.
- FISMA processes (i.e., annual self-assessments, FISMA metrics analysis) described in CIO-IT Security-04-26.
- Audits (e.g., IG, FISMA) performed on GSA's system and security processes.
- Incidents/Events identified by internal or external activities described in CIO-IT Security-01-02.

These processes provide key insight into how GSA's risk management strategy is performing. Effectiveness monitoring will also be performed by defining key performance metrics/indicators, defining acceptable thresholds for the indicators and measuring progress towards achieving the performance metrics.

Based on the analysis of the effectiveness of these risk management processes, metrics, and measures, GSA will modify them in order to reduce risks and improve information system and information security. Modifications may include, but is not limited to, the following types of actions:

- Increasing automation (e.g., CDM tools) in identifying vulnerabilities and risks;
- Modifying measures/metrics to increase expected levels of protection of systems and their data;
- Improving incident response and vulnerability detection capabilities by assessing new tools, technologies, and techniques and integrating them where appropriate;
- Focusing remediation/mitigation responses to address the highest risk/highest impact items first;
- Using lessons learned during response and recovery activities/tests to improve processes and techniques.