IT Security Procedural Guide: Annual FISMA and Financial Statements Audit Guide CIO-IT Security-22-121

Revision 1

May 15, 2023

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 – April 25, 2022		
N/A	Agosto/ Woodcock/ Klemens	Initial Release	Developed guide to standardize the process of supporting annual audits.	N/A
		Revision 1 – May 15, 2023		
1	McCormick	• Updated language regarding Office of Financial Management. • Updated format to align with current guidelines.	Requested by Office of Audit Management and Accountability.	3

Approval

IT Security Procedural Guide: Annual FISMA and Financial Statements Audit Guide, CIO-IT Security 22-121, Revision 1 is hereby approved for distribution.

DocuSigned by:
Bo Berlas
FD7170261615445...

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

List of Tables

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 web page or document listed in Section 1.4, References.

1 Introduction

The intent of Public Law 113-283, "Federal Information Security Modernization Act of 2014" (FISMA) is to protect government information and assets from unauthorized access, use, disclosure, disruption, modification, or destruction. FISMA is the law; the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5, "Security and Privacy Controls for Information Systems and Organizations," is the standard that contains the individual security controls required to comply with FISMA.

To comply with FISMA, General Services Administration (GSA) systems must implement the appropriate security controls from NIST SP 800-53 based on their security categorization. That categorization is determined by following the process in Federal Information Processing Standards (FIPS) Publication 199, "Standards for Security Categorization of Federal Information and Information Systems." GSA has added NIST SP 800-53 controls to its systems' baselines to more closely align with GSA's mission and business requirements, and environments of operation. The controls are implemented, assessed, and the overall risk of operating a GSA system determined as described in the Assessment and Authorization (A&A) process from NIST SP 800-37, "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy." Completing that process results in an Authorization to Operate (ATO) for a system.

Any GSA system may be the subject of annual audits by the GSA Office of the Inspector General (GSA OIG). These audits are generally broken down into two major categories and conducted by the GSA OIG and/or their designated contract auditors:

1. Annual FISMA Systems Audit.
2. Annual Financial Systems Audit.

These audits provide Congress, the Executive Branch, and GSA leadership with a regulated benchmark as to the security posture of each system chosen for auditing, measured against standards set forth in GSA OIG policy and Office of Management and Budget (OMB) annual security metrics and directives. These audits also outline potential risks, weaknesses, and areas of concern that might lie across all GSA systems.

1.1 Purpose

The purpose of this guide is to provide guidance on how GSA prepares for, supports, and analyzes the results of annual FISMA and Financial audits.

1.2 Scope

The requirements and methods outlined in this guide apply to any GSA system contained within GSA's system inventory. The requirements and methods outlined in this guide apply to all GSA Federal employees and contractors who have FISMA related responsibilities and oversight as outlined in GSA Order CIO 2100.1, "GSA Information Technology (IT) Policy." Per CIO 2100.1, a GSA system is a system:

- Used or operated by GSA; or
- Used or operated on behalf of GSA by a contractor of GSA or by another organization.

1.3 Policy

CIO 2100.1 requires all "GSA Federal employees, contractors, and vendors of GSA, who manage, maintain, operate, or protect GSA systems or data" to comply with the policies therein. Implementation of requirements from FISMA, OMB Circular A-130, "Managing Information as a Strategic Resource," supporting GSA's IT Security Program, and laws and Federal guidance regarding financial systems and privacy data is ingrained throughout CIO 2100.1. As such, the support of audits or independent assessments in support those Federal Laws and regulations is required by CIO 2100.1

1.4 References

Federal Laws, Standards, Regulations, and Publications:

- FIPS PUB 199, "Standards for Security Categorization of Federal Information and Information Systems"
- 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 800-53, Revision 5, "Security and Privacy Controls for Information Systems and Organizations"
- OMB Circular A-123, "Management's Responsibility for Enterprise Risk Management and Internal Control"
- OMB Circular A-130, "Managing Information as a Strategic Resource"
- Public Law 113-283, "Federal Information Security Modernization Act of 2014"

GSA Policies, Procedures, Guidance:

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

The following guides are available at gsa.gov on the IT Security Procedural Guides page. Although any guide listed on that page may be in scope for an audit, the guides listed below are the key guides describing how GSA identifies, manages, monitors, and remediates risks.

- CIO-IT Security-01-02: Incident Response (IR)
- CIO-IT Security-06-30: Managing Enterprise Cybersecurity Risk
- CIO-IT Security-09-44: Plan of Action and Milestones (POA&M)
- CIO-IT Security-09-48: Security and Privacy Requirements for IT Acquisition Efforts
- CIO-IT Security-11-51: Conducting Penetration Test Exercises
- CIO-IT Security-12-66: Information Security Continuous Monitoring (ISCM) Strategy and Ongoing Authorization (OA) Program
- CIO-IT Security-17-80: Vulnerability Management Process
- CIO-IT Security-18-91: Risk Management Strategy (RMS)
- CIO-IT Security-19-95: Security Engineering Architectural Reviews
- CIO-IT-Security-19-101: External Information System Monitoring
- CIO-IT Security-21-117: OCISO Cyber Supply Chain Risk Management (C-SCRM) Program

The following guides are available on GSA's IT Security Procedural Guides Insite page.

- CIO-IT Security-18-90: Common Control Catalog (CCC)

2 Roles and Responsibilities

The roles and responsibilities provided in this section have been extracted or paraphrased from CIO 2100.1 or summarized from GSA and Federal guidance. Throughout this guide, requirements for managing systems going through the annual FISMA and Financial audits are described. Complete roles and responsibilities for agency management officials and roles with significant IT Security responsibilities are defined in CIO 2100.1.

2.1 Chief Information Officer (CIO)

The GSA CIO has overall responsibility for the GSA IT Security Program and the conduct of GSA IT personnel in the preparation and conduct of the annual audits.

2.2 Office of the Chief Financial Officer (OCFO) Office of Audit Management and Accountability

The OCFO Office of Financial Management (BG) is the coordinating hub for GSA's annual financial statements audit and agency financial report. The Office of Audit Management and Accountability manages U.S. Government Accountability Office (GAO) and Office of Inspector General (OIG) performance audits and OIG contract audits.

2.3 GSA Chief Information Security Officer (CISO)

The CISO is the focal point for GSA IT security and must ensure the security requirements described in applicable regulations, orders and policies are implemented agency wide. The CISO has overall management responsibility for the security related areas of those GSA FISMA systems undergoing audit by the OIG and also for preparation for, support during the conduct of an audit, and follow-up actions after the audit.

2.4 Heads of Services and Staff Offices (HSSOs)

HSSOs are senior officials or executives within GSA with specific mission or line of business responsibilities. They are responsible for coordinating the efforts of management and technical personnel under their jurisdiction in meeting GSA IT Security requirements including preparation for audits, support during the conduct of audits, and post audit activities for systems under their purview selected for audit.

2.5 System Owner

System owners are management officials within GSA with responsibility for the acquisition, development, maintenance, implementation, and operation of GSA systems. System owners represent the interests of the system throughout its lifecycle and should provide resources required to prepare for, support the conduct of, and perform post audit activities for systems selected for audit that are under their purview.

2.6 OCISO Division Directors

OCISO Division Directors are the focal point for all IT system security matters, resources, and activities under their responsibility. Specific to audits, the Division Directors' responsibilities are:

- **Policy and Compliance Division (ISP) Director.** Responsible for developing and maintaining policy and oversight for all systems selected for audit and to maintain a current status of audits as they are conducted.
- **Staff Offices Division Director (IST) Director.** Responsible for ensuring Information Systems Security Officers (ISSOs) and Information Systems Security Managers (ISSMs) they complete processes and procedures necessary to prepare and submit requested artifacts in a timely manner and participate in the conducting of audits for their systems.
- **Other Division Directors.** Responsible for ensuring personnel in their divisions complete the processes or procedures necessary to prepare and submit requested artifacts in a timely manner and participate in the conducting of audits for areas under their purview.

2.7 ISSO and ISSM

ISSOs and ISSMs are responsible for performing or coordinating all actions required during the preparation and support of audits for systems under their purview. Their support is key to ensure all artifacts requested are provided for during the conducting of an audit as well as providing information updates on a regular basis to the GSA CISO and the Director of ISP and IST.

2.8 Infrastructure (DIGIT) Support Personnel and Government Equivalent

DIGIT Support Personnel and Government Equivalent are responsible for infrastructure related preparation prior to audit kickoff and timely submission of requested artifacts and information during the audit, including attendance at out briefs, for affected systems supported.

2.9 Audit Management Team

The Audit Management Team consists of personnel from the auditing entity and GSA personnel as listed below. Their responsibilities include the following:

1. Auditing Entity – Responsible for the notification of audit engagement, weekly status meetings, and conducting the overall audit.
2. ISP Division – Responsible for pre-audit functions; responding to requests for entity wide items; tracking and managing audit functions within the OCISO, to include, but not limited to reviewing audit response submissions; managing and tracking audit responses; monitoring Corrective Action Plan (CAPs) and obtaining necessary signoff.
3. ISSO and ISSM – Responsible for responding to data call requests for system specific items and working with stakeholders to gather responses.
4. Office of Deputy CIO (ID) – Responsible for coordination of meetings and collection of documentation.
5. IS Divisions – Responsible for responding to data call requests that are enterprise wide and working with stakeholders to gather responses.

3 Audit Types

Financial statement audits and FISMA audits are the two types of audits covered in this guide; a brief description of each audit type is provided in the following sections. Both types of audits use Provided By Client (PBC)/Meeting Request Lists (MRLs) and Document Request Lists (DRLs) to manage individual requests by the auditors during the course of the audit. The ISSM/ISSO or

other personnel as designated by the ISP Director provide the information as requested in PBC/MRLs and DRLs.

For both types of audits, a weekly audit status report is maintained to update all parties involved in the audit and includes potential findings for further discussion.

3.1 Financial Statement Audits

An annual financial statement audit is conducted in conjunction with the GSA internal audit branch, OCFO, and OIG. OCISO ISP Division staff coordinates with OCFO's Office of Audit Management and Accountability and acts as liaison between that office, other OCISO IS staff, and the auditors. Any systems included in the audit require support from the ISSOs and ISSMs of those systems. The ISSM-Enterprise Application and Infrastructure Support Branch (ISTE) supports physical walk-throughs of data centers by the auditors, as necessary.

3.2 Systems FISMA Audits

An annual FISMA audit is conducted by the GSA OIG to determine the maturity of GSA's security program and assess the compliance of selected FISMA systems with GSA's security program and A&A processes. The steps of the FISMA audit are:

1. Entrance conference between OIG and CIO.
2. Selection of systems to be audited by OIG.
3. Acceptance by CISO of selection - pending discussion with CIO.
4. Release of PBC list for each selected system.
5. Gather/submission of artifacts for PBC items (ISSO/ISSM).
6. Weekly internal meeting with ISSOs/ISSMs prior to weekly status meeting with auditors.
7. PBC meetings (OIG and all responsible parties), updates made by OIG to PBC.
8. Gather/submission of artifacts for updated PBC items (ISSO/ISSM).
9. Initial audit completion status meeting (OIG and CISO).
10. Ongoing meeting to resolve findings between OIG and CISO.
11. Review of draft audit report (OIG and CISO).
12. Exit conference (OIG and CISO).
13. Submission of DHS CyberScope metric by OIG.
14. Release of final report by OIG to CIO.

4 FISMA Audit Sequence

The following sections describe the events/activities that comprise a FISMA audit. Financial statement audits generally follow the same process as systems audits, except there is no self-assessment step.

4.1 Notification of Engagement

The auditing entity (e.g., OIG) starts an audit by providing a Notification of Engagement to the OCISO. It states the purpose, objectives, method, and logistics of the audit. Upon receipt of notification, the following additional activities occur for FISMA audits. Notifications for financial statement audits are to the OCFO, who then notifies the OCISO regarding systems in scope for the audit. For a financial statement audit, any steps described below are limited to the in-scope systems of the financial audit.

1. The auditing entity schedules a kickoff meeting.

2. ISP Director and designated personnel attend the kickoff meeting.
3. The auditing entity requests the FISMA system inventory.
4. The auditing entity provides a self-assessment spreadsheet based on maturity levels, typically 1-5, for each domain being audited. A self-assessment is not a part of financial statement audits.
5. ISP receives the list of systems selected for audit, reviews the list for suggested revisions, and sends any revisions to the auditor.
6. The auditors review the suggested revisions and issue a final list of systems to be audited.
7. Once the final list is received, audit preparation begins.

4.2 OIG Self-Assessment

GSA completes the OIG's annual self-assessment indicating GSA's determination of its maturity level for various security domains. Although the domains may be modified year-to-year, the domains listed below are the current domains.

- Risk Management
- Supply Chain Risk Management
- Configuration Management
- Identity and Access Management
- Data Protection and Privacy
- Security Training
- Information Security Continuous Monitoring (ISCM)
- Incident Response
- Contingency Planning

The ISP Director designates personnel (e.g., Directors, ISSMs/ISSOs, other IS staff) to complete the self-assessment spreadsheet based on their domain knowledge/responsibility for the specific domains being audited. The designated personnel use a self-assessment sheet which includes two summary sheets and tabs to rate GSA from 1-5 in each domain (with 5 being the highest) and provide justification, references, and artifacts, as necessary, to support the assigned ratings.

As the self-assessment is completed, a series of meetings occur with the designated personnel and the ISP Director to discuss the questions in the self-assessment and the maturity level ratings. Once the self-assessment is complete and receives concurrence from the CISO, the ISP Director provides it to the auditing entity.

4.3 Audit Preparation

The audit preparation tasks are completed prior to the audit to ensure readiness for the official audit (both Financial and FISMA). During the audit preparation phase, documents, scans, and certifications (e.g., user certifications) are examined to ensure that information is correct and up to date and to identify any deficiencies.

- ISP shares the list of systems to be audited with the points of contact (POCs).
- ISP holds a meeting with the ISSOs and ISSMs and prepares a Pre-Audit Checklist. The checklist is a living document that is updated annually to incorporate lessons learned from previous audits, current showstopper controls, previous audit findings, and current core metrics.

- The ISSOs and ISSMs populate the checklist with information including, but not limited to the following:
  - Review of all ATO showstoppers.
  - Evidence that vulnerability scan documentation is up to date, including execution, reviews, and reporting.
  - Evidence that the System Security and Privacy Plan (SSPP) and Security Assessment Report (SAR) documentation is timely and compliant.
  - Evidence that user certifications are current and complete.
  - Evidence that terminations are current and complete (within policy 30-day window).
  - Evidence that configuration management documentation is timely and complete.
  - Evidence that there is an inventory of all users and documented roles are current and complete.
- The ISSOs and ISSMs review the data listed above and continue the audit preparation via the pre-audit checklist for both internal and contractor systems.
  - An assessment of the systems selected is performed to look for previous findings or pain points and ensure they have been addressed.
  - Any deficiencies identified are reported to ISP and the ISSOs and ISSMs work with the program office to correct all deficiencies.
  - ISP is notified of the corrective actions taken for each deficiency and tracks these corrective actions.

If all deficiencies cannot be corrected by the time of the actual audit, ISP escalates the deficiencies to the Authorizing Official (AO) and CISO.

A portion of the FY23 pre-audit checklist is depicted in Table 4-1.

Table 4-1. Example of Pre-Audit Checklist

Item#	*Question/Checklist Item*	*ATO Showstoppers & Scan Results*	Date Verified	Verified By (Name)	Comments
1	Did the system have overdue (over 30 days) critical/High risk vulnerabilities from 10/01/2021 through current ?Does the system have any outstanding BOD 22-01 KEV vulnerabilities If yes, identify assets in scope, scan reports and selected dates plus any overdues. If any were discovered provide the POA&M's, AoR's, etc.				
2	Are all (100%) of assets being scanned for operating system vulnerabilities (weekly)?				
3	Are all URLs (100% in the inventory) being scanned for unauthenticated scans on the monthly scans?				
4	Are all production URLs (100% in the inventory) being scanned for authenticated scans on an annual basis?				
5	Does the system have any End-Of-Life (EOL) software that is no longer supported by the manufacturer?				
6	Does have system have MFA implemented for all unique ID's, password requirements that meets GSA's policy for all layers (OS, DB, and APP), and Separation of Duty conflicts?				

4.4 Discovery

Discovery is the data gathering phase for the auditors. The auditors issue FISMA PBC MRLs and DRLs to collect documents and request meetings. The steps during the discovery phase are listed below.

1. The auditing entity receives the maturity levels and assessments from ISP and begins discovery by creating and issuing the current entity-wide and system-specific FISMA PBC MRLs and DRLs.

2. ISP receives the current and prior year PBC MRLs and DRLs. These lists are not always received at the same time. Usually the current year is received first, and the prior year is received later in the process. Upon receipt of the lists, the following actions take place.
    - For both current and prior year lists, ISP responds to the items that are enterprise wide.
    - ISSOs and ISSMs respond to the system specific items for the current and prior year list.
    - ISP updates the PBC lists with GSA POCs and creates a list of enterprise-wide processes.
    - ISP schedules meetings with stakeholders for enterprise-wide walkthroughs.
    - ID, along with the ISSOs and ISSMs and other IS divisions, work with ISP to coordinate meetings and collect documentation that has been requested.
3. The auditing entity creates Google folders for the enterprise-wide and system-specific PBC lists. The folders contain:
    - Sheets identifying system-specific and enterprise-wide PBC lists.
    - PBC response folders for ISP or designated personnel to upload the requested documentation.
4. ISP submits the PBC list responses for enterprise-wide items to the auditors.
5. ISSOs and ISSMs submit PBC list responses for system specific items to the auditors.
6. ISP checks the system's teams PBC MRL and DRL status on a daily basis.

A portion of a PBC DRL list is depicted in Table 4-2. The MRL list is similar, with MRL Description replacing DRL Description and there is no NIST control in the MRL sheet.

Table 4-2. Example PBC/DRL List

FY 2021 GSA FISMA Document Request List (DRL)											
						Risk Management (RM)					
PY DRL #	Current DRL #	FISMA Metric	NIST Control	Maturity Level	Request Type	DRL Description	Date Requested	Due Date	Date Received	Date Accepted	Status
EW-RM-PBC-01	EW-RM-PBC-01	1.3	CA-3/ PM-5	3	Document	System generated listing of GSA information Systems.	N/A	N/A	N/A	N/A	Closed
EW-RM-PBC-02	EW-RM-PBC-02	2.3	CA-7/ CM-8	3	Selection	For the following selection of in-scope devices, inspect the tools and determine they are listed on the tools (Tenable Security Center, BigFix, Forescout). Please show the hardware assets for the following systems: - GECO - ROCIS II	6/9/2021	6/18/2021	6/21/2021	7/15/2021	Closed
EW-RM-PBC-03	EW-RM-PBC-03	2.3	CA-7/ CM-8	3	Selection	GSA Management's monthly review (ending the 15th) of November 2020 and May 2021 of the software and hardware inventory report.	6/9/2021	6/18/2021	6/21/2021	6/21/2021	Closed
EW-RM-PBC-04	EW-RM-PBC-04	3.3	CA-7/ CM-8	3	Selection	For the following selection of in-scope devices, inspect the tools to determine the software listed in SSP are captured and reported in the tools (Tenable Security Center and MaaS360). Please provide the software inventory report for the following hardware assets: Please refer to EW-RM-PBC-23 for this PBC request	N/A	N/A	N/A	N/A	Closed
EW-RM-PBC-05	EW-RM-PBC-05	4.3	RA-2/PM-7/PM -11	3	Selection	Meeting agendas and minutes to track management decisions for risk management that impact GSA. Please provide the minutes for the following weekly minutes: Refer to EW-RM-PBC-22 for documents	N/A	N/A	N/A	N/A	Closed
EW-RM-PBC-06	EW-RM-PBC-06	4.3	RA-2/PM-7/PM -11	3	Document	GSA's plan for implementing the Cybersecurity Framework within their Risk Management Strategy.	N/A	N/A	N/A	N/A	Closed
EW-RM-PBC-07	EW-RM-PBC-07	5.3	PM-8 / PM-9	3	Document	GSA's current risk profile as required per OMB Circular A-123 approved by management and GEO Risk Register	6/9/2021	6/18/2021	6/23/2021	6/25/2021	Closed

The PBC DRL sheet depicted consists of:

Column A - PY DRL # - Prior Year DRL Number.

Column B - Current DRL # - Current Year DRL Number

Column C - FISMA Metric - FISMA Metric Number. The FISMA metric listed is associated with the DRL identified.

Column D - NIST Control – The NIST controls associated with the FISMA metric and the DRL identified.

Columns E-O: Maturity Level, Request Type, DRL Description, Date Requested, Due Date, Date Received, Date Accepted, Status, Assigned POC, KPMG Comments, GSA Comments.

4.5 Field Work and Notification of Findings and Recommendations (NFRs)

Field work is generally a deeper dive into selected areas accompanied by additional questions with greater specificity. During this phase, Notification of Findings and Recommendations (NFRs) are issued. NFRs are issued by auditors to identify weaknesses in the agency's systems or processes. NFRs can be new findings or may be reissued findings if a weakness or inefficiency noted in the NFR was identified during a prior year audit but was not corrected by the time of the new audit. The fieldwork and creation of NFRs, in general, consists of the following steps.

1. Once all DRLs and MRLs are completed, the auditors analyze the collected data and notify ISP of potential findings.
2. ISP then notifies the impacted POCs, AOs, ISSOs/ISSMs and system owners of these potential findings.
3. The auditors issue draft NFRs for review.
4. ISP receives the draft NFRs, reviews them, and shares the data with the AO and system owners.
5. ISP provides comments or questions to the draft NFRs and sends the responses on the findings to the auditors.
6. The auditors receive the responses, review them, and send the final NFRs to ISP.
7. ISP receives the final NFRs, reviews them, and sends them to responsible parties for signoff:
    - If the NFRs are system specific, they are sent to the AO and the CISO.
    - If the NFRs are enterprise wide, they are sent to the CISO for signoff.
8. Once signoff is obtained, ISP sends the signed NFRs to the auditors.
9. ISP works with ISSMs and ISSOs, and others as necessary, to coordinate the development of Corrective Action Plans (CAPs) addressing the NFRs.

4.6 Reporting and Exit Conference

There are three reports issued as a result of the FISMA audit: a CyberScope report, a Public IG report, and a Restricted IG report. Once these reports have been issued the exit conference takes place. The exit conference formally closes the field work and analysis activities. The timeline for the issuance of the draft and final report is provided at this time.

1. Once the auditors receive the signed NFRs, they issue the CyberScope draft report.
2. ISP receives the CyberScope report and provides comments or corrections to the auditors.
3. The auditors receive the comments and corrections from ISP and populate CyberScope.
4. The auditors then issue the public and restricted draft IG reports.
5. ISP receives both reports, reviews them, and provides comments.
6. The auditors receive the comments from ISP and issue the final IG report.
7. ISP provides management responses as well as schedules and holds the exit conference.

8. ISP holds lessons learned sessions to discuss what went well and items to improve on from the audit.
9. The auditors issue the final public and restricted IG reports to ISP and the audit is concluded.

4.7 Post Audit Actions

The post-audit review process focuses on ensuring all NFRs have been addressed (i.e., there is a plan to resolve issues requiring corrective action). CAPs include actions taken and the resultant outcome for each NFR. Supporting documentation provides evidence showing that the results and outcomes resolve NFRs. All evidentiary artifacts are to be uploaded to the specified folder using established naming conventions. All CAPs must be completed 30 days prior to the next audit cycle.