



**IT Security Procedural Guide:
External Information System
Monitoring
CIO-IT Security-19-101**

Revision 1

March 12, 2020

Office of the Chief Information Security Officer

VERSION HISTORY/CHANGE RECORDS

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
		Initial Release – October 22, 2019		
N/A	IST	New guide created		
		Revision 1 – March 12, 2020		
N/A	Klemens	Updated ISSO Checklist due dates, clarified deliverable review/acceptance process, added usage of Archer for ISSO checklists. Updated process workflow diagram.	Update to reflect current GSA guidance and clarify deliverable review/acceptance process.	Multiple

Approval

IT Security Procedural Guide: External Information System Monitoring, CIO-IT Security-19-101, Revision 1, is hereby approved for distribution.

X DocuSigned by:
Bo Berlas
ED717926161544E

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

1	Introduction	1
1.1	Purpose	1
1.2	Scope.....	1
1.3	References	1
2	Roles and Responsibilities.....	2
2.1	GSA Chief Information Security Officer (CISO).....	2
2.2	Authorizing Officials (AO).....	2
2.3	Office of CISO Division Directors (OCISO)	2
2.4	Information Systems Security Manager (ISSM)	2
2.5	Information System Security Officer (ISSO)	2
2.6	System Owner	3
2.7	Contracting Officer/Contracting Officer Representative (CO/COR)	3
3	Deliverable Requirements.....	3
3.1	Quarterly Deliverables	3
3.2	Annual Deliverables	4
3.3	Biennial Frequency Deliverables	4
4	Deliverable Submission and Review Timelines.....	4
4.1	Vendor Submissions.....	5
4.2	Review Process.....	5
4.3	Tracking and Monitoring Reviews.....	6
5	External Information System Monitoring Process	6
5.1	Vendor Requirements	7
5.2	CO/COR Requirements.....	8
5.3	ISSO Requirements	8
5.4	ISSM Requirements.....	8
5.5	System Management	8
6	Storage of A&A Artifacts	9
	Appendix A – Related Artifacts	11
	Figure 5-1: Process Workflow	7
	Table 6-1: Deliverable Locations and Frequencies	9

NOTE: Hyperlinks in this guide are provided as follows:

- Section 1.3 References - This section contains hyperlinks to Federal Regulations/Guidance and to GSA webpages containing GSA policies, guides, and forms.

Note: 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

Many of the General Services Administration's (GSA) Information Technology (IT) systems are external information systems. While GSA does not have day-to-day operational responsibility for securing these systems, Public Law 113-283, "*Federal Information Security Modernization Act of 2014*" (FISMA) places ultimate responsibility for security with GSA. This requires developing processes to ensure adequate oversight, including having the correct contracting language outlined in CIO-IT Security-09-48, "*Security and Privacy Requirements for IT Acquisition Efforts*" and ensuring that deliverables are provided timely and meet requirements outlined within this document.

1.1 Purpose

This procedural guide defines the processes and procedures that will be used to ensure that external information systems are monitored, and that required deliverables are provided timely and meet GSA security requirements.

1.2 Scope

The requirements outlined within this guide apply to all GSA Federal employees, contractors, and vendors who oversee/protect GSA information systems and data. The guide provides GSA Federal employees, contractors, and vendors as identified in GSA Order CIO 2100.1, "GSA Information Technology (IT) Security Policy", and other IT personnel involved in the oversight of external information systems, the specific processes to follow for properly accomplishing oversight of external information systems under their purview.

1.3 References

Note: GSA updates its IT security policies and procedural guides on independent biennial cycles which may introduce conflicting guidance until revised guides 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.

Federal Laws, Regulations, and Guidance:

- [Public Law 113-283](#), "*Federal Information Security Modernization Act of 2014*"

GSA Guidance:

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

The guidance documents below are available on the GSA IT Security [Procedural Guides InSite](#) page.

- CIO-IT Security-09-48, "*Security and Privacy Requirements for IT Acquisition Efforts*"
- CIO-IT Security-09-44, "*Plan of Actions and Milestones (POA&M)*"

2 Roles and Responsibilities

There are many roles associated with external information system monitoring. The roles and responsibilities in this section have been extracted or paraphrased from CIO 2100.1 or summarized from GSA and Federal guidance.

2.1 GSA Chief Information Security Officer (CISO)

- Implementing and overseeing GSA's IT Security Program by developing and publishing security policies and IT security procedural guides.
- Establishing reporting deadlines for IT Security related issues requiring an agency response affecting the GSA IT Security Program.
- 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.
- Supporting the GSA CIO in reporting to the GSA Administrator on the effectiveness of the agency information security program, including progress of remedial actions.

2.2 Authorizing Officials (AO)

- Reviewing and approving security safeguards of information systems and issuing ATO approvals for each information system under their purview based on the acceptability of the security safeguards of the system (risk-management approach);
- Providing support to the ISSMs and ISSOs appointed by the GSA CISO for GSA systems under their purview.

2.3 Office of CISO Division Directors (OCISO)

- Monitoring adherence and proper implementation of GSA's IT Security Policy and reporting the results to the CISO.

2.4 Information Systems Security Manager (ISSM)

- Ensuring A&A support documentation is developed and maintained for the life of the system.
- Ensuring adherence and proper implementation of GSA's IT Security Policy.

2.5 Information System Security Officer (ISSO)

- Ensuring the system is operated, used, maintained, and disposed of IAW documented security policies and procedures.
- Performing the recurring activities as listed in the ISSO Checklist¹.

¹ The external information systems checklist identified in Archer should be used by ISSOs for any external information systems and resolves any conflicts between the referenced ISSO checklist and CIO-IT Security-09-48.

2.6 System Owner

- 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 A&A of the system to include security planning, risk assessments, security and incident response testing, configuration management, and contingency planning and testing.

2.7 Contracting Officer/Contracting Officer Representative (CO/COR)

- 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 include the security contract language from GSA CIO-IT Security-09-48.

3 Deliverable Requirements

There are three types of deliverables in monitoring external information systems at GSA, categorized by frequency: Quarterly, Annual, and Biennial. Unless specified otherwise within this guide, the creation, management, and reporting of each deliverable type is the same. Deliverables that can be attested to by the vendor of the external information system are identified with an "*" in the following sections.

3.1 Quarterly Deliverables

The following deliverables will be submitted on a quarterly basis.

- Web Application Vulnerability Scan Reports
- Operating System Vulnerability scan Reports
- Plan of Action & Milestones (POA&M) Update

Note: GSA's parameter for RA-5, Vulnerability Scanning, requires vulnerability scanning of operating systems-including databases weekly, and for web applications unauthenticated scans monthly, and authenticated scans annually.

3.2 Annual Deliverables

The following deliverables will be submitted on an annual basis.

- System Security Plan
- Contingency Plan
- User Certification/Authorization Review Documents
- *Separation of Duties Document/Matrix
- *Information Security Awareness and Training Records
- Annual FISMA Self-Assessment
- *System(s) Baseline Configuration Standard Document
- System Configuration Settings Verification
- Configuration Management Plan
- Contingency Plan Test Report
- Incident Response Test Report
- Information System Interconnection Agreements
- *Rules of Behavior
- Penetration Test Report
- *Personnel Screening and Security

*Attestation acceptable in Annual Attestation Statement

3.3 Biennial Frequency Deliverables

The following deliverables will be submitted on a biennial basis.

- *Access Control Policy and Procedures
- *Security Awareness and Training Policy and Procedures
- *Audit and Accountability Policy and Procedures
- *Identification and Authentication Policy and Procedures
- *Incident Response Policy and Procedures
- *System Maintenance Policy and Procedures
- *Media Protection Policy and Procedures
- *Physical and Environmental Policy and Procedures
- *Personnel Security Policy and Procedures
- *System and Information Integrity Policy and Procedures
- *System and Communication Protection Policy and Procedures
- *Key Management Policy

*Attestation acceptable in Biennial Attestation Statement

4 Deliverable Submission and Review Timelines

Submission dates are used to ensure adequate time is allowed for creation, review and corrective action, and reporting. Submission dates will align with the Federal Fiscal Year (FY)

(October 1 – September 30). The FY quarters end on the last day of December, March, June, and September. Annual and Biennial dates coincide with the end of September (biennial aligned with even years (e.g., 2020, 2022)).

4.1 Vendor Submissions

The [Vendor Security Deliverable Quality Checklist](#) is used to ensure all supporting artifacts meet GSA requirements, including documents identified in vendor attestation statements. The vendor is encouraged to use the quality checklist to verify their deliverables meet GSA's requirements. The GSA ISSO uses the quality checklist to validate that the deliverables are acceptable. Deliverable submissions are due as indicated below.

- Quarterly Artifacts/Deliverables are due 1 month prior to the completion of each quarter. Due dates are the last workday of the months listed:
 - **Quarter 1 – November**
 - **Quarter 2 – February**
 - **Quarter 3 – May**
 - **Quarter 4 – August**
- Annual Vendor Attestation Statements with supporting artifacts are due 2 months prior to completion of the fiscal year. Due date is the last workday of:
 - **July**
- Biennial Vendor Attestation Statements are due 2 months prior to completion of the fiscal year in which they are due. Due date is the last workday of:
 - **July (on even years: 2020, 2022, 2024, etc.)**

4.2 Review Process

The deliverables submission and review process is depicted in Figure 5-1 and is summarized in the Steps below.

Step 1A and 1B. The vendor produces the required deliverables, including vendor attestation letters, as appropriate. The deliverables are then delivered to GSA.

Step 2A and 2B. The GSA ISSO and CO/COR review the deliverables and based on contractual requirements and the [Vendor Security Deliverable Quality Checklist](#) determine their acceptability.

Step 2C. The GSA ISSO and ISSM use the Contractor ISSO Checklists implemented in GSA's Archer Governance, Risk, and Compliance (GRC) to document reviews and actions based on those reviews.

Steps 3, 4A, and 4B. If there are issues with the deliverables the ISSO coordinates with the vendor to correct minor issues. Major issues are coordinated between the ISSO and ISSM. Any

issues resulting in non-compliance (checklist and attestation letter) will be handled through the POA&M process as defined in CIO-IT Security-09-44, “*Plan of Actions and Milestones (POA&M)*.”

Step 4A and 5. The ISSM reviews deliverables and coordinates with the vendor/ISSO to correct any minor issues, major issues that cannot be resolved are handled via the system’s POA&M.

Step 6. Archer GRC is used to report on status and for ISSMs and others to analyze the data for possible process improvements.

4.3 Tracking and Monitoring Reviews

Quarterly, Annual, and Biennial Contractor ISSO Checklists have been implemented in GSA’s Archer GRC system for vendor deliverables. These checklists are used by ISSOs to document deliverable reviews and actions taken based on those reviews. Checklist campaigns are created based on the frequency of the deliverables and assigned to ISSOs who receive an email notification. ISSOs complete a checklist and submit it in Archer which generates an email to ISSMs indicating a checklist has been submitted for their review and approval. ISSMs approve or reject submitted checklists. ISSOs review rejected checklists and coordinate with the ISSM and the vendor to address any issues until a checklist is able to be resubmitted and approved.

5 External Information System Monitoring Process

The following diagram depicts the workflow associated with the external information system monitoring process.

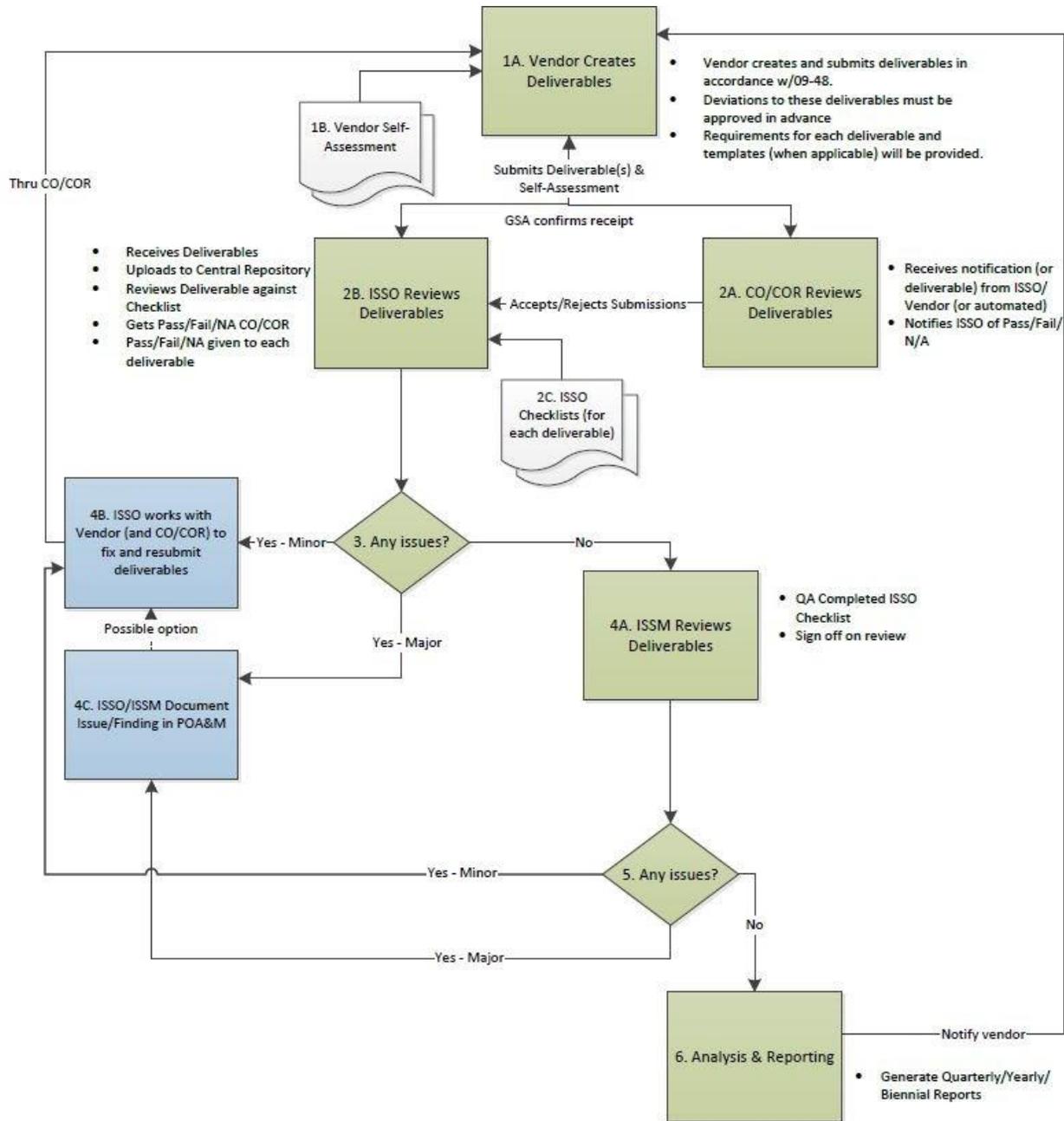


Figure 5-1: Process Workflow

5.1 Vendor Requirements

The vendor is responsible for providing all deliverables/artifacts that meet or exceed the checklist criteria on or before the submission date. Any questions or concerns should be discussed with the ISSO and/or CO/COR.

The vendor should submit the documents to both the CO/COR and the ISSO and if sent by email the artifacts should be encrypted.

5.2 CO/COR Requirements

The CO/COR is responsible for reviewing the contractor submissions as it deems fit. The CISO's office will not prescribe a checklist for the CO/COR.

The CO/COR is required to notify the ISSO with their acceptance or rejection of the submissions, so their information is included for the ISSM review.

5.3 ISSO Requirements

The ISSO is responsible for ensuring timely submission by the vendor as well as ensuring that the submission meets the requirements identified in the checklist.

The ISSO will identify any issues with the submissions and will work with vendor and CO/COR to adjust the submissions prior to the end of the ISSO review period. If adjustments are made, the ISSO checklists should be updated and the adjusted submissions should be stored on the Team Drive.

Prior to the ISSO finalizing their review, they need confirmation from the CO/COR that a review was performed. If any issues were observed, the ISSO must report that information to the ISSM.

The ISSO can, at any time, elevate items or issue. The ISSO should initially attempt to elevate items to the ISSM, but they may also, as necessary, include the System Owner, Authorizing Official, or CISO.

The ISSO is responsible for disseminating checklists to the vendor POCs.

5.4 ISSM Requirements

The ISSM will perform a quality assurance check on the ISSM checklist items and review the submissions for additional security concerns. For each submission period, the ISSM will evaluate the system for risk based on the submissions and prior issues, to include POA&M items. If the ISSM does not find any significant issues, they will approve the checklist for that period.

The ISSM is responsible for ensuring the ISSO has access to the latest checklists and recommending updates to the checklists and overall process.

When issues are observed, the ISSM will take action appropriate for the risk. Any issues resulting in non-compliance (checklist and attestation letter) will be handled through the POA&M process as defined in CIO-IT Security-09-44, "*Plan of Actions and Milestones (POA&M)*."

5.5 System Management

System Management (including Authorizing Official and System Owner) will typically be involved on a periodic basis through the reporting process for status and lower risk issues.

System management will also be involved on an ad hoc basis as higher risk issues arise. Minimally, reporting will be quarterly and yearly, unless a more frequent reporting frequency is required.

Ad hoc issues will usually be reported from the ISSO to the ISSM. The ISSM will report to the office of the CISO. Depending on the nature of the issue, one or more of the following roles will likely be brought in to assist in resolving the issue: Authorizing Official, System Owner, CO/COR, ISSM, ISSO, or vendor staff.

6 Storage of A&A Artifacts

A&A artifacts must be stored in the location and frequency identified below.

Table 6-1: Deliverable Locations and Frequencies

Deliverable	Frequency	Storage Location	Covered in Attestation Statement
Web Application vulnerability scan reports	Quarterly	Google Drive	No
Operating System (including databases) vulnerability scan reports	Quarterly	Google Drive	No
Plan of Action & Milestones (POA&M) Update	Quarterly	Google Drive	No
System Security Plan	Annual	Archer GRC	No
Contingency Plan	Annual	Archer GRC	No
User Certification/Authorization Review Documents	Annual	Archer GRC	No
Separation of Duties Document/Matrix	Annual	Archer GRC	Yes
Information Security Awareness and Training Records	Annual	Archer GRC	Yes
Annual FISMA Self-Assessment	Annual	Archer GRC	No
System(s) Baseline Configuration Standard Document	Annual	Archer GRC	Yes
System Configuration Settings Verification	Annual	Archer GRC	No
Configuration Management Plan	Annual	Archer GRC	No
Contingency Plan Test Report	Annual	Archer GRC	No
Incident Response Test Report	Annual	Archer GRC	No
Information System Interconnection Agreements	Annual	Archer GRC	No
Rules of Behavior	Annual	Archer GRC	Yes
Penetration Test Report	Annual	Archer GRC	No
Personnel Screening and Security	Annual	Archer GRC	Yes
Access Control Policy and Procedures	Biennial	Archer GRC	Yes
Security Awareness and Training Policy and	Biennial	Archer GRC	Yes

Procedures			
Audit and Accountability Policy and Procedures	Biennial	Archer GRC	Yes
Identification and Authentication Policy and Procedures	Biennial	Archer GRC	Yes
Incident Response Policy and Procedures	Biennial	Archer GRC	Yes
System Maintenance Policy and Procedures	Biennial	Archer GRC	Yes
Media Protection Policy and Procedures	Biennial	Archer GRC	Yes
Physical and Environmental Policy and Procedures	Biennial	Archer GRC	Yes
Personnel Security Policy and Procedures	Biennial	Archer GRC	Yes
System and Information Integrity Policy and Procedures	Biennial	Archer GRC	Yes
System and Communication Protection Policy and Procedures	Biennial	Archer GRC	Yes
Key Management Policy	Biennial	Archer GRC	Yes

Appendix A – Related Artifacts

Below are documents that are maintained separate from this procedural guide:

Stakeholder list by system. This Google Sheet identifies the ISSM, ISSO, System Owner, Authorizing Official, Contracting Officer, and Contracting Officer Representative for GSA external information systems. Please contact the system's ISSO or ISSM if access to the Google Sheet or information from it is needed.

The following forms/templates are available on the [IT Security Procedural Forms](#) page.

- **External Information System ISSO Checklist**
- **Vendor Security Deliverable Quality Checklist (Quarterly)**
- **Vendor Attestation Statement (Annual)**
- **Vendor Attestation Statement (Biennial)**