GSA IT

IT Security Procedural Guide: Audit and Accountability (AU) CIO-IT Security-01-08

Revision 7

February 21, 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
		Revision 2 – January 29, 2008		
1	Scott/Heard	Changes made throughout the document to reflect FISMA, NIST and GSA CIO P 2100.1B requirements.	Updated to reflect and implement various FISMA, NIST and GSA CIO P 2100.1B requirements.	Various
2	Scott/Heard	Changes throughout the document to correspond with revisions made to CIO-IT Security-10-09, CIO-IT Security-01-03 and CIO-IT Security-01-04.	Updated to reflect the correlation of the CIO-IT Security Guides; and to further express policy within them as standalone documents	Various
3	Hummel/ Windelberg	Changes throughout the document to correspond with update of the current version of GSA CIO P 2100 and other updates	Update to the most current version of GSA CIO P 2100 and provide more detailed guidance on implementing policy.	Various
		Revision 3 – June 30, 2010		
1	Berlas/Cook	Changes throughout the document to correspond with update of the current version of GSA CIO P 2100 and NIST 800-53 rev3.	Update to the most current version of GSA CIO P 2100 and provide more detailed guidance on implementing policy.	Various
		Revision 4 – March 22, 2017		
1	Wilson/ Yardley/ Klemens	Changes throughout the document to correspond with update of the current version of NIST 800-53 Rev4.	Update to NIST 800-53, Rev 4 and correlate with GSA Guidance on parameters and implementation.	Various
		Revision 5 – November 3, 2017		
1	Feliksa/ Heffron/ Klemens	Updated format and NIST SP 800-53 control parameters and incorporated current Federal regulations and guidance.	Incorporate most current Federal regulations, NIST guidance, and GSA requirements.	Various
		Revision 6 – December 2, 2020		
1	Sibley/ Weaver/ Klemens/ Dean	Revised to address: • Updated control parameters and implementation details, especially regarding the ELP. • Added information identifying controls as common, hybrid, or system-specific. • Added a section regarding NIST SP 800-161 SCRM controls. • Updated to current format and style, including Section 508 compliance. • Revised how the CSF is related to audit and accountability.	Update to current Federal, NIST, and GSA regulations, guidance, and requirements.	Various
		Revision 7 – February 21, 2023		

1	Yardley/ McCormick/ Klemens/ Quintananieves	Revisions included: • Updated to NIST SP 800-53, Revision 5 controls, GSA parameters, and implementation statements. • Updated format and content.	Align to current NIST and GSA guidance and GSA parameters. New or substantively changed controls in Revision 5 are: AU-2, AU-3(3), AU-5, AU-6(1), AU-9.	Throughout
2	Yardley/ McCormick/ Klemens/ Quintananieves	Revisions included: • Provided three control sections for different types of systems. • Adjusted implementation details to align with SecTools CRM.	Aligned to allow types of systems to determine their requirements more easily.	Throughout

Approval

IT Security Procedural Guide: Audit and Accountability (AU), CIO-IT Security 01-08, Revision 7, is hereby approved for distribution.

DocuSigned by:
Bo Berlas
FD717926161544F...

Bo Berlas
GSA Chief Information 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 for external sources can be found in Appendix C.
- It may be necessary to copy and paste hyperlinks found in this document (Right-Click, Select Copy Hyperlink) directly into a web browser rather than using Ctrl-Click to access them within the document.
- This guide is provided in three distinct sections; (1) Federal systems integrated with the SecTools Enterprise Logging Platform (ELP), (2) Federal systems not in integrated with ELP, and (3) Vendor/Contractor systems. Since readers may only read the section applicable to them acronyms are established in each section.

1 Introduction

Audit trails maintain a record of system activity both by system and application processes and by user activity of systems and applications. When complemented with appropriate tools and procedures, audit trails can provide a means to help accomplish several security-related objectives, including but not limited to: (1) establishing individual accountability; (2) detecting security violations and intrusions; (3) identifying flaws in systems and applications; (4) performing problem analysis; and (5) assisting in incident reconstruction.

When auditing is not implemented, is improperly configured, and/or the resultant audit logs are not regularly reviewed, the following outcomes may occur in the event of a system compromise:

- An incident may go undetected;
- An attacker may hide their location, malicious software, and activities on the compromised host;
- User accountability for actions may be unsupported;
- System changes may not be noticed.

If a compromise is detected, without properly protected and complete logging records, those charged with the security responsibility for the system are blind to the details of the attack. The attack may go unnoticed, with attackers sometimes controlling compromised machines for months or years without anyone in the organization knowing, even though the evidence of the attack has been recorded in unexamined log files. Audit records may be the only evidence of a successful attack.

Although assessed as part of a system’s Assessment and Authorization (A&A) process, audit logging cannot be just for compliance purposes. Audit logs must be used for proactive review, including real-time analysis, ongoing periodic reviews, and to establish what occurred after an event. Reviewers should know what to look for to effectively spot unusual activity and understand the normal activity for the systems under their purview.

Every General Services Administration (GSA) system must follow the practices described in this guide. Any deviations from the security requirements established in GSA CIO Order 2100.1, “GSA Information Technology (IT) Security Policy,” must be coordinated by the appropriate Information Systems Security Officer (ISSO) through the appropriate Information Systems Security Manager (ISSM) and approved by the Authorizing Official (AO). Any deviations, exceptions, or other conditions not following GSA policies and standards must be submitted using the Security Deviation Request Google Form.

This guide provides guidance for the AU security controls identified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5, “Security and Privacy Controls for Information Systems and Organizations.” This guide provides an overview of auditing, auditing roles and responsibilities, NIST SP 800-53 audit and accountability requirements per Federal Information Processing Standards (FIPS) Publication 199, “Standards for Security Categorization of Federal Information and Information Systems," security categorization level and system type, and procedures for implementing these requirements.

Executive Order (EO) 13800, "Presidential Executive Order on 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). GSA uses the NIST SP 800-37, "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy," commonly referred to as the Risk Management Framework (RMF) as its foundation for managing risk, including the implementation of NIST SP 800-53 controls. Further information on how AC controls relate to the CSF is provided in Appendix A.

1.1 Purpose

The purpose of this guide is to provide guidance for the AU security controls identified in NIST SP 800-53 and audit and accountability requirements specified in CIO Order 2100.1. The guide provides GSA Federal employees, contractors with significant security responsibilities (as identified in CIO Order 2100.1), and other IT personnel involved in implementing AU controls, the specific procedures they are to follow for implementing auditing and logging features and functions for systems under their purview.

1.2 Scope

The requirements outlined within this guide apply to and must be followed by all GSA Federal employees and contractors who are involved in implementing, administering, managing, or monitoring the audit and accountability controls of GSA systems and information. All GSA systems must adhere to the requirements and guidance provided with regard to the procedures, processes, and methods for auditing and accountability as described in this guide. 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

Appendix B contains the CIO 2100.1 policy statements regarding auditing and logging for GSA systems.

1.4 References

Appendix C provides links to references used throughout this guide.

2 Roles and Responsibilities

There are many roles associated with implementing effective auditing and logging, and reviews of the records produced. System owners for each information system are responsible for ensuring that auditing and accountability processes exist for their specific systems and that the appropriate personnel have been assigned AU control activities/tasks to satisfy the control requirements. Appendix D provides a listing of roles and responsibilities related to implementing, administering, managing, monitoring, and reviewing auditing and logging at GSA.

3 GSA SecTools Implementation of the Enterprise Logging Platform

GSA Security Tools (SecTools) is a Federal Information Security Modernization Act (FISMA) system managed by the GSA SecOps team and other teams. It is a collection of commercial off the shelf software (COTS) tools that provide different security services.

The GSA Enterprise Logging Platform (ELP) is part of the SecTools system. It is operated by the SecOps Team to provide support to GSA systems for logging, log review, and security monitoring. The ELP is a Cloud-based platform fed from multiple GSA security tools, devices, agents, and operating systems.

Although “SecTools” and “ELP” may be used interchangeably in some cases, this guide will use “ELP” for consistency.

3.1 Implementation of OMB M-21-31 Requirements

OMB M-21-31, “Improving the Federal Government’s Investigative and Remediation Capabilities Related to Cybersecurity Incidents,” addresses the requirements for information system logging, log retention, and log management, including the ability to centrally access logs to enable visibility before, during, and after cybersecurity incidents.

Table 3-1 provides a timeline for systems’ compliance with OMB M-21-31 requirements. Details are provided in the sections below.

Table 3-1. M-21-31 Compliance Timeline

System Type	Target Date
Federal System Integrated with the ELP	Next ATO renewal or two years from the signature date on this guide, whichever comes last.
Federal System Not Integrated with the ELP (includes new systems)	Within one year of its signed ATO or two years from the signature date on this guide, whichever comes last.
Contractor Systems - Current	Next ATO renewal or two years from the signature date on this guide, whichever comes last.
Contractor Systems - New	Within one year of a signed ATO.

Systems in GSA's Ongoing Authorization Program	Within two years from the signature date on this guide.

3.2 Federal Information Systems

All GSA systems are Federal Information systems. CIO 2100.1 further classifies systems based on the following definitions, which are used throughout this guide.

- **Contractor System.** An information system in GSA's inventory processing or containing GSA or Federal data where the infrastructure and applications are wholly operated, administered, managed, and maintained by a contractor in non-GSA facilities.
- **Federal System (i.e., Agency System).** An information system in GSA's inventory processing or containing GSA or Federal information where the infrastructure and/or applications are NOT wholly operated, administered, managed, and maintained by a Contractor.

Timelines all systems to comply with the requirements in M-21-31 are in Table 3-1.

3.2.1 Federal Systems Integrated with the ELP

Federal systems integrated with the ELP are afforded time to comply with M-21-31 requirements in order to budget resources to support the compliance effort. Until systems implement M-21-31 they are considered compliant if they meet the control requirements as detailed in Section 5. Federal systems must consult with SecOps and consider M-21-31 compliance when making major changes to their systems, including but not limited to tooling used to review and analyze log data.

Note: If a GSA system is integrated with the ELP and does not contain any Personally Identifiable Information (PII)/sensitive (e.g., financial, Controlled Unclassified Information [CUI]) data, several of its audit logging requirements are satisfied by inheriting those controls from SecTools and fulfilling the responsibilities in the SecTools Customer Responsibilities Matrix (CRM). Integration with SecTools means that GSA security agents and SecTools logging configuration and/or agents are installed.

3.2.2 Federal Systems Not Integrated with the ELP (including new systems)

Existing federal systems not currently integrated with the ELP must consult SecOps and consider M-21-31 compliance when making major changes to their systems, including but not limited to tooling used to review and analyze log data.

3.2.3 Contractor Systems (Current and New)

Contractor systems are responsible for conducting a gap analysis for their systems' audit logging solution against M-21-31 and creating a project plan to bring the system into compliance with the mandate. Contractor systems should coordinate this project with their ISSO, ISSM, and the GSA IST Director.

4 Control Implementation Guidance for AU Controls

In the implementation guidance text, the GSA-defined parameter settings included in the control requirements are in blue, italicized text and offset by brackets. As stated in Section 1.2, Scope, the requirements outlined within this guide apply to all GSA systems and must be followed by all GSA Federal employees and contractors involved in implementing audit and accountability of GSA systems and information. The GSA implementation guidance stated for each control applies to personnel and/or the systems operated by or on behalf of GSA. Instructions and requirements are provided in the following sections:

- Section 5: Federal systems integrated with the ELP;
- Section 6: Federal systems not integrated with the ELP, including new systems;
- Section 7: Contractor systems.

Table 4-1 identifies the designation of all AU controls as common, hybrid, or system specific controls for both Federal and contractor systems. Effectively, common controls are provided by GSA at the enterprise level or by one of GSA's Major Information Systems (previously General Support Systems), system specific controls are implemented at the system level, and hybrid controls have shared responsibilities for control implementation. CIO-IT Security-18-90: Information Security Program Plan (ISPP), describes the GSA enterprise-wide controls and outlines the responsible parties for implementing them.

Note: The ISPP is being updated to NIST SP 800-53, Revision 5, at the same time as this guide. Contact ispcompliance@gsa.gov for guidance if there is a discrepancy between this guide and the ISPP.

Table 4-1: Designation of AU Controls

System Type/ Control Type	Federal Systems	Contractor Systems
Common	AU-1	
Hybrid	AU-4, AU-5, AU-6, AU-6(1), AU-6(3), 6(4), AU-7, AU-7(1), AU-9, AU-9(4), AU-11 **Note: Hybrid only for systems integrated with the ELP. For systems not integrated with the ELP these controls are system specific.**	AU-1
System-Specific	AU-2, AU-3, AU-3(1), AU-3(3), AU-5(1), AU-5(2), AU-6(5), AU-6(6), AU-8, AU-9(2), AU-9(3), AU-10, AU-12, AU-12(1), AU-12(3)	AU-2, AU-3, AU-3(1), AU(3), AU-4, AU-5, AU-5(1), AU-5(2), AU-6, AU-6(1), AC-6(3), AC-6(4), AU-6(5), AU-6(6), AU-7, AU-7(1), AU-8, AU-9, AU-9(2), AU- 9(3), AU-9(4), AU-10, AU-11, AU-12, AU-12(1), AU-12(3)

Table 4-2 identifies GSA AU control applicability at the FIPS 199 Low, Moderate, and High levels.

Table 4-2: AU Control Applicability

FIPS 199 Level/A&A Process	Applicable Controls
Low	AU-1, AU-2, AU-3, AU-4, AU-5, AU-6, AU-8, AU-9, AU-11, AU-12
Moderate	AU-1, AU-2, AU-3, AU-3(1), AU-3(3)^, AU-4, AU-5 AU-6, AU-6(1), AU-6(3), AU-6(4)**, AU-7, AU-7(1), AU-8, AU-9, AU-9(4), AU-11, AU-12
High	AU-1, AU-2, AU-3, AU-3(1) , AU-3(3)^, AU-4, AU-5, AU-5(1), AU-5(2), AU-6, AU-6(1), AU-6(3), AU-6(4)**, AU-6(5), AU-6(6), AU-7, AU-7(1), AU-8, AU-9, AU-9(2), AU-9(3), AU-9(4), AU-10, AU-11, AU-12, AU-12(1), AU-12(3)
LATO	AU-2, AU-6(1)
MiSaaS	AU-2, AU-3, AU-6, AU-6(1), AU-11

**-control is applicable at the level listed per GSA OCISO Tailored Moderate Baseline
^-control is applicable if PII is stored, processed, or transmitted

For readers' ease of use, "mini tables" (see example below) that contain control/enhancement designation and applicability information is provided at the end of control statements for each AU control. The tables allow readers to see if a control/enhancement is applicable at their system's FIPS Level/A&A process and if it is common (C), Hybrid (H), or system specific (S), eliminating the need to refer back to Tables 4-1 and 4-2 for this information.

	Low	Mod	High	LATO	MiSaaS	Federal	Contractor
Control ID	✓	✓	✓			C	H

5 Federal Systems Currently Integrated with the ELP

The SecOps team operates the ELP to provide support to GSA systems for logging, log review, and security monitoring. This platform is part of the SecTools FISMA system. As such, personnel managing systems currently integrated with the ELP will be referred to the SecOps Team and SecTools CRM for details throughout this document, as appropriate.

Systems deployed within the GSA on-premise network or the Federal Acquisition Service (FAS) Cloud Services (FCS) FISMA system in Amazon Web Services (AWS) can leverage the ELP and inherit parts of several NIST controls from the SecTools FISMA system to reduce their own responsibilities. The hybrid nature of these controls requires the ISSO and system personnel to work with the SecOps team to configure agents and document how the customers' responsibilities for the controls are being met.

If a GSA system is integrated with SecTools and does not contain any PII or sensitive (e.g., financial, CUI) data, several of its audit logging requirements are satisfied by inheriting those controls and fulfilling the SecTools customer responsibilities. Integration with SecTools means that GSA security agents and SecTools logging configuration and/or agents are installed. For a list of the inherited and hybrid controls provided by SecTools, reference the SecTools CRM

Spreadsheet. Teams wanting to inherit from SecTools must be on-boarded by SecOps using the Log Forward/Collection On-board Request form.

5.1 AU-1 Audit and Accountability Policy and Procedures

Control:

a. Develop, document, and disseminate to [*personnel with IT security responsibilities as defined in GSA Order CIO 2100.1*]:
   1. [*Organization-level*] audit and accountability policy that:
      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
   2. Procedures to facilitate the implementation of the audit and accountability policy and the associated audit and accessibility controls;

b. Designate an [*CISO*] to manage the development, documentation, and dissemination of the audit and accessibility policy and procedures; and

c. Review and update the current audit and accessibility:
   1. Policy [*annually, as part of CIO 2100.1 update*] and following [*changes to Federal or GSA policies, requirements, or guidance*]; and
   2. Procedures [*at least every three (3) years*] and following [*changes to Federal or GSA policies, requirements, or guidance*].

	Low	Mod	High	LATO	MiSaaS	Federal
AU-1	✓	✓	✓			C

Common Control Implementation
GSA's audit and accountability policy is defined in the GSA IT Security Policy, CIO 2100.1, which addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance regarding audit and accountability for GSA systems. This policy is maintained to be consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines by updating the policy via Changes, Instructional Letters, or the annual update as applicable. This policy is disseminated via the Directives Library webpages at GSA.gov and GSA InSite.

GSA's audit and accountability procedures are documented in CIO-IT Security-01-08, Audit and Accountability (AU) [this guide]. The procedures facilitate the implementation of the audit and accountability policy and associated controls. This guide is disseminated GSA-wide via IT Security Procedural Guides webpages on GSA.gov and GSA's InSite websites.

Per 2100.1, the CISO is responsible for managing the development and publishing of all security policies and IT security procedural guides. The GSA OCISO is responsible for reviewing and updating CIO 2100.1 annually. The GSA OCISO is responsible for reviewing and updating CIO-IT

Security-01-08 at least every three years and following changes to Federal or GSA policies, requirements, or guidance.

GSA Service and Staff Offices (SSOs) or system owners may augment the access control policies and procedures included in 2100.1 and CIO-IT Security-01-08 to address additional organizational or system-specific auditing and accountability requirements. Any such policies and procedures must establish timeframes for updating them.

5.2 AU-2 Event Logging

Control:

a. Identify the types of events that the system is capable of logging in support of the audit function: [
   (1) *successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events;*
   (2) *Web applications should log all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes;*
   (3) *for technologies with limited auditing features, the capabilities will be recommended by the GSA SSO or Contractor, based on an industry source such as vendor guidance or Center for Internet Security benchmark, and approved by the GSA CISO and AO*];
b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged;
c. Specify the following event types for logging within the system: [
   (1) *audit configuration requirements as documented in applicable GSA IT Security Technical Guides and Standards (i.e., hardening and technology implementation guides)*
   (2) *for web applications see GSA IT Security Procedural Guide 07-35, Section 2.8.10, What to Log*
   (3) *for technologies where a Technical Guide and Standard does not exist, events from an industry source such as vendor guidance or Center for Internet Security benchmark, recommended by the GSA SSO or Contractor and approved by the GSA CISO and AO*];
d. Provide a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and
e. Review and update the event types selected for logging [*annually or whenever there is a change in the system's threat environment as communicated by the GSA SSO AO or the GSA OCISO*].

	Low	Mod	High	LATO	MiSaaS	Federal
AU-2	✓	✓	✓	✓	✓	S

Enterprise Logging Platform (ELP) Integration Requirements
The GSA SecOps team operates the ELP; system owners may forward operating system auditable events to it. The customer's (i.e., system owners/personnel) responsibilities for leveraging the SecTools environment are detailed in the SecTools CIS/CRM. The system personnel in collaboration with the system ISSO/ISSM review the selected event types for logging annually as part of the SSPP review and update, or if the system's threat environment changes.

The GSA SecOps team uses host-based security agents and the ELP to correlate operating system auditable events which may trigger alerts on security events which are further analyzed and correlated with other security systems in the ELP. FISMA system owners should request to have host-based security agents installed on an individual operating system and, if supported, host-based security agent events will be forwarded to the ELP. These security events are maintained, managed, and correlated by SecOps and reviewed in the ELP by the ISO Division's Security Operations Center (SOC). ISSOs retain the responsibility of verifying that logging is correctly configured and processed in accordance with the control statement.

For events from components the ELP does not support (e.g., database, application) and until all M-21-31 requirements are supported by the ELP, the ISSO must coordinate with the System Owner to ensure the AU-2 controls are met.

Regarding the selection of events to be audited, GSA has created a series of system hardening guides and associated benchmarks that are available on the IT Security Technical Guides and Standards webpage, these guides define the configuration of audit events to support GSA operations.

5.3 AU-3 Content of Audit Records

Control:

Ensure that audit records contain information that establishes the following:

a. What type of event occurred;
b. When the event occurred;
c. Where the event occurred;
d. Source of the event;
e. Outcome of the event; and
f. Identity of any individuals, subjects, or objects/entities associated with the event.

Control Enhancements:

(1) Content of Audit Records | Additional Audit Information. Generate audit records containing the following additional information: [

i. Session, connection, transaction, or activity duration;

- ii. *For client-server transactions, the number of bytes received and bytes sent. This gives bidirectional transfer information that can be helpful during an investigation or inquiry;*
- iii. *For client-server transactions, unique metadata or properties about the client initiating the transaction. This could include properties such as an IP address, user name, session identifier, or browser characteristics (e.g., a 'User-Agent' string).*
- iv. *Details regarding the event 'type': the type of method (for HTTP: GET/POST/HEAD, etc.) or action (Database INSERT, UPDATE, DELETE);*
- v. *Characteristics that describe or identify the object or resource being acted upon; and*
- vi. *Additional informational messages to diagnose or identify the event].*

(3) Content of Audit Records | Limit Personally Identifiable Information Elements. Limit personal identifiable information contained in audit records to the following elements identified in the privacy risk assessment: [*no PII to be included in audit records*].

	Low	Mod	High	LATO	MiSaaS	Federal
AU-3	✓	✓	✓		✓	S
AU-3(1)		✓	✓			S
AU-3(3)		✓^	✓^			S

^-control is applicable if PII is stored, processed, or transmitted

Guidance for Systems Integrated With the ELP

System teams are responsible for ensuring the required content of audit records is captured and forwarded to the ELP. System owners/teams are responsible for ensuring PII data and sensitive data, such as financial data, are not stored or shipped in logs. PII and sensitive data may not be sent to the ELP even if they are encoded.

5.4 AU-4 Audit Log Storage Capacity

Control:

Allocate audit log storage capacity to accommodate [*GSA policies and guidance: audit log sizes are documented in applicable GSA IT Security Technical Guides and Standards (i.e., hardening and technology implementation guides) available on the IT Security Technical Guides and Standards webpage*].

	Low	Mod	High	LATO	MiSaaS	Federal
AU-4	✓	✓	✓			H

Guidance for Systems Integrated with the ELP

Table 3-3 identifies, at the various system layers, which logs should be stored locally and/or forwarded when integrated with the ELP.

Table 5-1. Log Storage

System Layers	Store Logs Locally^	Forward Logs^
Cloud Service Provider (e.g., AWS)	X*	X
Operating Systems	X*	X
Databases	X*	X
Applications	X*	X
Tools	X*	X
Security Agent/Device Events		X

^When logs are shipped to the ELP they should continue to be stored locally for 60 days. On day 61, they can be deleted.

*****These logs are required to be shipped to the ELP when required based on complying with M-21-31. See Section 3.1 of this document

Local Log Storage: Logs should be stored by the system team, either on the host itself or in a storage repository (i.e., the team has access to options such as network-attached storage or S3). The storage type used must be durable to avoid loss of audit logs. Per control AU-11, logs must be retained for a minimum of 12 months online and 18 months in cold storage by the end of FY24. This timeline allows systems to grow audit logs since this is a recent change from the previous requirement of 6 months for log retention.

5.5 AU-5 Response to Audit Logging Process Failures

Control:

a. Alert [*the GSA Enterprise Security Operation Center (SOC) via the ELP for systems integrated with it; Administrators (Application, System, Network, etc.) for systems not integrated with the ELP*] within [*GSA SSO or Contractor recommended time period as approved by the GSA CISO and AO*] in the event of an audit logging process failure; and
b. Take the following additional actions: [*shut down information system, overwrite oldest audit records, or stop generating audit records*].

Control Enhancements:

(1) Response to Audit Logging Process Failures | Storage Capacity Warning. Provide a warning to [*Administrators (Application, System, Network, etc.)*] within [*GSA SSO or Contractor recommended time period as approved by the GSA CISO and AO*] when allocated audit log storage volume reaches [*GSA SSO or Contractor recommended percentage as approved by the GSA CISO and AO*] of repository maximum audit record storage capacity.
(2) Response to Audit Logging Process Failures | Real-Time Alerts. Provide an alert within [*GSA SSO or Contractor recommended time period as approved by the GISA CISO and AO*] to [*the GSA ISO Division via the ELP for systems integrated with the ELP, Administrators (Application, System, Network, etc.) for systems not integrated with the ELP*] when the following audit failure events occur: [*GSA SSO or Contractor*

recommended audit failure events requiring real-time alerts as approved by the GSA CISO and AO].

	Low	Mod	High	LATO	MiSaaS	Federal
AU-5	✓	✓	✓			H
AU-5(1)			✓			S
AU-5(2)			✓			S

Guidance for Systems Integrated with the ELP
An alert to the GSA SOC will be generated on audit log process failures for systems integrated with the ELP.

For control AU-5, part b, systems will have to take one of the actions listed in its parameter upon audit processing failure.

For enhancement AU-5(1), systems will have to configure warnings for the roles/personnel within the system's specified timeframe, when the system's specified percentage of capacity for log storage is reached.

For enhancement AU-5(2), systems will have to configure alerts within the system's specified time period to the system's specified personnel when the system's specified alerts occur.

Additional details regarding ELP and customer responsibilities related to the base control can be found in the SecTools CIS/CRM.

5.6 AU-6 Audit Record Review, Analysis, and Reporting

Control:

a. Review and analyze system audit records [*Systems integrated with the ELP where automated analysis and correlations is performed: on business days; otherwise on a periodic or event driven basis (periodicity or events driving reviews are recommended by the GSA SSO or Contractor and approved by the GSA CISO and AO)*] for indications of [*GSA SSO or Contractor recommended inappropriate or unusual activity as approved by the GSA CISO and AO*] and the potential impact of the inappropriate or unusual activity;
b. Report findings to [*ISSM, ISSO, System Owner, Custodian, as designated and approved by the GSA CISO and AO, via a dashboard when events are forwarded to the ELP, otherwise via an alternative automated or manual reporting mechanisms*]; and
c. Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.

Control Enhancements:

(1) Audit Record Review, Analysis, and Reporting | Automated Process Integration. Integrate audit record review, analysis, and reporting processes using [*the GSA ELP for*

systems integrated with it; GSA SSO or Contractor recommended automated mechanisms as approved by the GSA CISO and AO].

(3) Audit Record Review, Analysis, and Reporting | Correlate Audit Record Repositories. Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.

(4) Audit Record Review, Analysis, and Reporting | Central Review and Analysis. Provide and implement the capability to centrally review and analyze audit records from multiple components within the system.

(5) Audit Record Review, Analysis, and Reporting |Integrated Analysis of Audit Records. Integrate analysis of audit records with analysis of [*information system monitoring information; GSA SSO or Contractor recommended data/information collected from other sources as approved by the GSA CISO and AO*] to further enhance the ability to identify inappropriate or unusual activity.

(6) Audit Record Review, Analysis, and Reporting | Correlation With Physical Monitoring. | Correlate information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity.

	Low	Mod	High	LATO	MiSaaS	Federal
AU-6	✓	✓	✓		✓	H
AU-6(1)		✓	✓	✓	✓	H
AU-6(3)		✓	✓			H
AU-6(4)		✓**	✓**			H
AU-6(5)			✓			S
AU-6(6)			✓			S

**-control is applicable at the level listed per GSA OCISO Tailored Moderate Baseline

Table 5-2 identifies, at the various system layers, who is responsible for reviewing logs.

Table 5-2. Log Review Responsibility

System Layers	Review Responsibility: Integrated with ELP
Cloud Service Provider (e.g., AWS)	SecOps (Only Reviewed Under Incident)
Operating Systems	SecOps (Only Reviewed Under Incident)
Log types requiring review only if PII or sensitive data (e.g., financial, CUI) is in scope: • Databases • Applications • Tools	System Team
Security Agent/Device Events	SecOps

Guidance for Systems Integrated With the ELP
For systems integrated with the ELP, aggregated and correlated logs and security-related events within the ELP are reviewed by ISO Division for indicators of compromise (e.g., inappropriate or unusual activity) on business days and, when identified, this activity will be evaluated for potential impact. If these reviews indicate a possible compromise that is not already indicated in an alert, on a dashboard, or via manual or automated hunting exercises, the GSA ISO division will initiate a manual report. When information (e.g., from law enforcement, intelligence, or other credible sources) warrants a change in risk, the level of audit review, analysis, and reporting is adjusted accordingly.

For enhancement AU-6(1), audit record review, analysis, and reporting processes are integrated in the ELP.

For enhancement AU-6(3), situational awareness across the organization is gained by analyzing and correlating audit records across multiple repositories via the ELP.

For enhancement AU-6(4), audit records from multiple systems can be centrally reviewed and analyzed within the ELP.

For enhancements AU-6(5) and AU-6(6), as requested by system personnel or others, the ISO Division will coordinate with the GSA Incident Response Team to integrate analysis from other sources while suspicious activities are investigated.

Additional details regarding ELP and customer responsibilities related to AU-6 and enhancements (1), (3), and (4) can be found in the SecTools CIS/CRM.

Systems Hosting PII/Sensitive Data
For systems hosting PII or sensitive (e.g., financial, CUI) data, system personnel assigned by the system owner, are responsible for conducting reviews for anomalous activity for layers identified in Table 5-2. A list of specific anomalous activities for a system with PII or sensitive (e.g., financial, CUI) should be identified for review and analysis based on targeted review tasks. Examples include:

- Unusual authentication and authorization events;
- Unauthorized data or content manipulation;
- Excessive web application or database activity; and
- Unauthorized or unusual transactions.

Teams must define their own approach for conducting review of these events and activities, at a frequency accepted and approved by the AO. It is not necessary for every team to deploy their own centralized tool such as a SIEM to comply with this guide. Teams can construct an approach which covers audit log review within specific applications, tools, and databases that form their system.

Methods that could be used for audit log review include:

- Creating a roster for audit log review that assigns one team member to this function every week;
- Creating a form to certify that audit log review has been conducted on a given day/week by a specific member of the team. For example, a Google Form can be used.

5.7 AU-7 Audit Record Reduction and Report Generation

Control:

Provide and implement an audit record reduction and report generation capability that:

a. Supports on-demand audit record review, analysis, and reporting requirements and after-the-fact investigations of incidents; and
b. Does not alter the original content or time ordering of audit records.

Control Enhancements:

(1) Audit Record Reduction and Report Generation | Automatic Processing. Provide and implement the capability to process, sort, and search audit records for events of interest based on the following content: [*Source IP, Destination IP, Account Names, Date and Time of Events, Event Type*].

	Low	Mod	High	LATO	MiSaaS	Federal
AU-7		✓	✓			H
AU-7(1)		✓	✓			H

Guidance for Systems Integrated with the ELP

The ELP supports retrievable records for audit review, analysis, reporting, and after-the-fact investigations of security incidents; it is configured to aggregate logs and can be configured to generate reports as required. Content and/or time ordering of audit records is not able to be altered.

Given the high volume of audit records collected, records of a similar nature may be aggregated such that only a subset of the data is retained, such as time of first and last event, number of events, along with the associated and relevant data points, if the majority of the data is identical.

For enhancement AU-7 (1), the ELP can process logs that have been forwarded to it based on parameters that include source IP, destination IP, account names, time and date of events and event type.

5.8 AU-8 Time Stamps

Control:

a. Use internal system clocks to generate timestamps for audit records; and
b. Record time stamps for audit records that meet [*GSA SSO or Contractor recommended granularity of time measurement to be approved by the GSA CISO and AO*] and that use

Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp.

	Low	Mod	High	LATO	MiSaaS	Federal
AU-8	✓	✓	✓			S

Guidance for Systems Integrated With the ELP
Platforms and systems must be configured to:

- Generate timestamps based on internal system clocks;
- Meet the approved granularity of time specified in the system SSPP; and
- Use or have offset information allowing timestamps to be mapped to Coordinated Universal time.

5.9 AU-9 Protection of Audit Information

Control:

a. Protect audit information and audit logging tools from unauthorized access, modification, and deletion; and
b. Alert [*the GSA Incident Response Team*] upon detection of unauthorized access, modification, or deletion of audit information.

Control Enhancements:

(2) Protection of Audit Information | Store on Separate Physical Systems or Components. Store audit records [*at least weekly, unless the data is being sent to a secondary system, e.g., the Enterprise Logging Platform,*] in a repository that is part of a physically different system or system component than the system or component being audited.
(3) Protection of Audit Information | Cryptographic Protection. Implement cryptographic mechanisms to protect the integrity of audit information and audit tools.
(4) Protection of Audit Information | Access by Subset of Privileged Users. Authorize access to management of audit logging functionality to only [*privileged users specifically authorized to perform audit management functions (i.e., specified administrators of applications, systems, networks, etc.)*].

Note: ISSOs, ISSMs, and System Owners may be provided read access to audit data; however, they will not have access to audit management functions.

	Low	Mod	High	LATO	MiSaaS	Federal
AU-9	✓	✓	✓			S
AU-9(2)			✓			S
AU-9(3)			✓			S
AU-9(4)		✓	✓			S

Guidance for Systems Integrated With the ELP

Access to events in the ELP is restricted to users authorized by the ISO Division and/or the system ISSO or ISSM. Within individual FISMA systems, the system owner must restrict access to local audit records to authorized personnel as designated by the ISSO/ISSM. Should unauthorized system use occur, including unauthorized access, modification, or deletion of audit information, the GSA IR Team must be informed.

For AU-9 and AU-9(4), when systems are integrated with the ELP, access to audit events is restricted to users authorized by the ISO Division and/or the system ISSO or ISSM. Platforms must restrict access to audit events to users authorized by the platform ISSO or ISSM.

For AU-9(2), the ELP provides backup of audit logs for systems integrated with it sufficient to support retention requirements in AU-11. However, AU-9(2) is applicable only the FIPS 199 High systems and the ELP does not receive logs from any FIPS 199 High systems.

For AU-9(3), similarly, since the ELP does not receive logs from any FIPS 199 High systems and AU-9(3) is only applicable to FIPS 199 High systems the ELP does not support the encryption of audit information and tools.

5.10 AU-10 Non-Repudiation

Control:

Provide irrefutable evidence that an individual (or process acting on behalf of an individual) has performed [*system specific actions, e.g., such as electronically signing a document, approving a request, or receiving a message*].

	Low	Mod	High	LATO	MiSaaS	Federal
AU-10			✓			S

Platform/system/application System Owners are responsible for ensuring system specific actions are not able to be reputed after they have occurred. Configuring platforms/systems/applications per the settings established in the Security Engineering (ISE) Division's Technical Guides and Standards assists in establishing non-repudiation capabilities. Some additional methods supporting non-repudiation include digital signatures and message receipts.

5.11 AU-11 Audit Record Retention

Control:

Retain audit records for [*12 months online and 18 months in cold storage*] to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements.

***Note:** Systems will have until the end of FY24 to allow time for captured logs to grow to the timeframes listed.*

	Low	Mod	High	LATO	MiSaaS	Federal
AU-11	✓	✓	✓		✓	H

Guidance for Systems Integrated With the ELP

Systems integrated with the ELP will have their forwarded audit records stored for at least 12 months in an online state and 18 months in a cold state. These retention requirements were recently extended from the prior 180-day retention requirement to comply with M-21-31. It will take at least 24 months before GSA systems meet this retention timeframe because newly ingested data has to grow over time. Such records are required to be simultaneously retained at the log source for 60 days.

5.12 AU-12 Audit Record Generation

Control:

a. Provide audit record generation capability for the event types defined in AU-2 a. on [*all components*];
b. Allow [*ISSMs, ISSOs, System Owners, Custodians*] to select the event types that are to be logged by specific components of the system; and
c. Generate audit records for the event types defined in AU-2 c, which includes the audit record content defined in AU-3.

Control Enhancements:

(1) Audit Record Generation | System-Wide and Time-Correlated Audit Trail. Compile audit records from [*all components*] into a system-wide (logical or physical) audit trail that is time correlated to within [*1 minute of UTC*].
(3) Audit Record Generation | Changes by Authorized Individuals. Provide and implement the capability for [*Administrators (Application, System, Network, etc.), ISSOs, ISSMs, System Owners*] to change the logging to be performed on [*all components*] based on [*change management decisions*] within [*minutes*].

	Low	Mod	High	LATO	MiSaaS	Federal
AU-12	✓	✓	✓			S
AU-12(1)			✓			S
AU-12(3)			✓			S

GSA systems must be able to generate audit records for the auditable events specified in AU-2.a with the content in AU-3 for all system components. System Owners, Custodians, ISSOs, and ISSMs must collaborate on which specific events are to be audited by specific components.

Platforms, including the cloud service provider layer where applicable, must coordinate with systems and applications they support to ensure that components at the platform level meet the AU-12 requirement.

Table 5-3 contains examples of system components and the logs associated with them that are capable of generating audit records.

Table 5-3. Examples of System Component Logs

System Components	Logs
Cloud Service Provider (e.g., AWS, Azure, etc.)	• Cloud Trail • CloudWatch logs (if used for security alerting) • VPC Flow logs
Operating Systems	• Linux/UNIX • Windows
Databases	• Oracle • MySQL • PostgreSQL • Others
Applications	• Apache • Drupal • WordPress • Solr • Security agents • Others
Tools	• Jenkins • Tableau • Others
Security Agent/Device Events	• Bit9 • ClamAV • Others

For enhancement AU-12(1), audit records must be time correlated to within 1 minute of UTC.

For enhancement AU-12(3), on a case-by-case basis, coordination between the ISO and ISE Divisions, System Owners, and ISSOs/ISSMs can identify recommended changes to system auditing and, following the system's change management process, system personnel can adjust auditing as necessary.

6 Federal Systems Not Integrated with the ELP (including new systems)

6.1 AU-1 Audit and Accountability Policy and Procedures

Control:

a. Develop, document, and disseminate to [*personnel with IT security responsibilities as defined in GSA Order CIO 2100.1*]:
   1. [*Organization-level*] audit and accountability policy that:
      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the audit and accountability policy and the associated audit and accessibility controls;

b. Designate an [*CISO*] to manage the development, documentation, and dissemination of the audit and accessibility policy and procedures; and

c. Review and update the current audit and accessibility:

1. Policy [*annually, as part of CIO 2100.1 update*] and following [*changes to Federal or GSA policies, requirements, or guidance*]; and
2. Procedures [*at least every three (3) years*] and following [*changes to Federal or GSA policies, requirements, or guidance*].

	Low	Mod	High	LATO	MiSaaS	Federal
AU-1	✓	✓	✓			C

Common Control Implementation

GSA's audit and accountability policy is defined in the GSA IT Security Policy, CIO 2100.1, which addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance regarding audit and accountability for GSA systems. This policy is maintained to be consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines by updating the policy via Changes, Instructional Letters, or the annual update as applicable. This policy is disseminated via the Directives Library webpages at GSA.gov and GSA InSite.

GSA's audit and accountability procedures are documented in CIO-IT Security-01-08, Audit and Accountability (AU) [this guide]. The procedures facilitate the implementation of the audit and accountability policy and associated controls. This guide is disseminated GSA-wide via IT Security Procedural Guides webpages on GSA.gov and GSA's InSite websites.

Per 2100.1, the CISO is responsible for managing the development and publishing of all security policies and IT security procedural guides. The GSA OCISO is responsible for reviewing and updating CIO 2100.1 annually. The GSA OCISO is responsible for reviewing and updating CIO-IT Security-01-08 at least every three years and following changes to Federal or GSA policies, requirements, or guidance.

GSA Service and Staff Offices (SSOs) or system owners may augment the access control policies and procedures included in 2100.1 and CIO-IT Security-01-08 to address additional organizational or system-specific auditing and accountability requirements. Any such policies and procedures must establish timeframes for updating them.

6.2 AU-2 Event Logging

Control:

a. Identify the types of events that the system is capable of logging in support of the audit function: [
   (1) *successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events;*
   (2) *Web applications should log all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes;*
   (3) *for technologies with limited auditing features, the capabilities will be recommended by the GSA SSO or Contractor, based on an industry source such as vendor guidance or Center for Internet Security benchmark, and approved by the GSA CISO and AO*];
b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged;
c. Specify the following event types for logging within the system: [
   (1) *audit configuration requirements as documented in applicable GSA IT Security Technical Guides and Standards (i.e., hardening and technology implementation guides)*
   (2) *for web applications see GSA IT Security Procedural Guide 07-35, Section 2.8.10, What to Log*
   (3) *for technologies where a Technical Guide and Standard does not exist, events from an industry source such as vendor guidance or Center for Internet Security benchmark, recommended by the GSA SSO or Contractor and approved by the GSA CISO and AO*];
d. Provide a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and
e. Review and update the event types selected for logging [*annually or whenever there is a change in the system's threat environment as communicated by the GSA SSO AO or the GSA OCISO*].

	Low	Mod	High	LATO	MiSaaS	Federal
AU-2	✓	✓	✓	✓	✓	S

Guidance for Systems Not Integrated with the ELP

For systems not integrated with the ELP, the ISSO must coordinate with the System Owner/team to ensure the AU-2 controls are met. These actions include:

- coordinating event logging with other organization entities (e.g., the ISO and ISE Divisions) to inform event selection;
- configuring logging/auditing functions to log events based on GSA hardening guides and web application security guide, and establishing approved logging for technologies where no GSA guide exists;
- documenting the rationale for why the selected events are adequate to support investigations; and

- reviewing the selected events annually as part of the SSPP review and update, or if the system's threat environment changes.

Regarding the selection of events to be audited, GSA has created a series of system hardening guides and associated benchmarks that are available on the IT Security Technical Guides and Standards webpage, these guides define the configuration of audit events to support GSA operations.

6.3 AU-3 Content of Audit Records

Control:

Ensure that audit records contain information that establishes the following:

a. What type of event occurred;
b. When the event occurred;
c. Where the event occurred;
d. Source of the event;
e. Outcome of the event; and
f. Identity of any individuals, subjects, or objects/entities associated with the event.

Control Enhancements:

(1) Content of Audit Records | Additional Audit Information. Generate audit records containing the following additional information: [

i. Session, connection, transaction, or activity duration;
ii. For client-server transactions, the number of bytes received and bytes sent. This gives bidirectional transfer information that can be helpful during an investigation or inquiry;
iii. For client-server transactions, unique metadata or properties about the client initiating the transaction. This could include properties such as an IP address, user name, session identifier, or browser characteristics (e.g., a 'User-Agent' string).
iv. Details regarding the event 'type': the type of method (for HTTP: GET/POST/HEAD, etc.) or action (Database INSERT, UPDATE, DELETE);
v. Characteristics that describe or identify the object or resource being acted upon; and
vi. Additional informational messages to diagnose or identify the event].

(3) Content of Audit Records | Limit Personally Identifiable Information Elements. Limit personal identifiable information contained in audit records to the following elements identified in the privacy risk assessment: [*no PII to be included in audit records*].

	Low	Mod	High	LATO	MiSaaS	Federal
AU-3	✓	✓	✓		✓	S
AU-3(1)		✓	✓			S
AU-3(3)		✓^	✓^			S

^-control is applicable if PII is stored, processed, or transmitted

Guidance for Systems Not Integrated With the ELP
The System Owner/team is responsible for ensuring the required content of audit records is captured.

For enhancement AU-3(1), the System Owner/team is responsible for ensuring that the system is configured to properly generate the additional information required by GSA's parameter.

For enhancement AU-3(3), the System Owner/team are responsible for ensuring PII data and sensitive data, such as financial data, are not stored in logs.

6.4 AU-4 Audit Log Storage Capacity

Control:

Allocate audit log storage capacity to accommodate [*GSA policies and guidance: audit log sizes are documented in applicable GSA IT Security Technical Guides and Standards (i.e., hardening and technology implementation guides) available on the IT Security Technical Guides and Standards webpage*].

	Low	Mod	High	LATO	MiSaaS	Federal
AU-4	✓	✓	✓			S

Guidance for Systems Not Integrated With the ELP
Logs should be stored by the system team either on the host itself or in a storage repository (i.e., the team has access to options such as network-attached storage or S3). The storage type used must be durable to avoid loss of audit logs. Per control AU-11, logs must be retained for a minimum of 12 months online and 18 months in cold storage by the end of FY24. This timeline allows systems to grow audit logs since this is a recent change from the previous requirement of 6 months for log retention.

6.5 AU-5 Response to Audit Logging Process Failures

Control:

a. Alert [*the GSA Enterprise Security Operation Center (SOC) via the ELP for systems integrated with it; Administrators (Application, System, Network, etc.) for systems not integrated with the ELP*] within [*GSA SSO or Contractor recommended time period as approved by the GSA CISO and AO*] in the event of an audit logging process failure; and
b. Take the following additional actions: [*shut down information system, overwrite oldest audit records, or stop generating audit records*].

Control Enhancements:

(1) Response to Audit Logging Process Failures | Storage Capacity Warning. Provide a warning to [*Administrators (Application, System, Network, etc.)*] within [*GSA SSO or Contractor recommended time period as approved by the GSA CISO and AO*] when allocated audit log storage volume reaches [*GSA SSO or Contractor recommended percentage as approved by the GSA CISO and AO*] of repository maximum audit record storage capacity.

(2) Response to Audit Logging Process Failures | Real-Time Alerts. Provide an alert within [*GSA SSO or Contractor recommended time period as approved by the GISA CISO and AO*] to [*the GSA ISO Division via the ELP for systems integrated with the ELP, Administrators (Application, System, Network, etc.) for systems not integrated with the ELP*] when the following audit failure events occur: [*GSA SSO or Contractor recommended audit failure events requiring real-time alerts as approved by the GSA CISO and AO*].

	Low	Mod	High	LATO	MiSaaS	Federal
AU-5	✓	✓	✓			S
AU-5(1)			✓			S
AU-5(2)			✓			S

Guidance for Systems Not Integrated with the ELP

The System Owner/team must configure alerts to be sent within the system’s specified time period to the system’s specified personnel in the event of audit log process failures and systems will have to take one of the actions listed in the AU-5, part b, parameter upon audit processing failure.

For enhancement AU-5(1), systems will have to configure warnings for the roles/personnel within the system’s specified timeframe, when the system’s specified percentage of capacity for log storage is reached.

For enhancement AU-5(2), systems will have to configure alerts within the system’s specified time period to the system’s specified personnel when the system’s specified alerts occur.

The GSA CISO and AO must approve all warning and alert parameters.

6.6 AU-6 Audit Record Review, Analysis, and Reporting

Control:

a. Review and analyze system audit records [*Systems integrated with the ELP where automated analysis and correlations is performed: on business days; otherwise on a periodic or event driven basis (periodicity or events driving reviews are recommended by the GSA SSO or Contractor and approved by the GSA CISO and AO)*] for indications of [*GSA SSO or Contractor recommended inappropriate or unusual activity as approved by the GSA CISO and AO*] and the potential impact of the inappropriate or unusual activity;
b. Report findings to [*ISSM, ISSO, System Owner, Custodian, as designated and approved by the GSA CISO and AO, via a dashboard when events are forwarded to the ELP, otherwise via an alternative automated or manual reporting mechanisms*]; and
c. Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.

Control Enhancements:

(1) Audit Record Review, Analysis, and Reporting | Automated Process Integration. Integrate audit record review, analysis, and reporting processes using [*the GSA ELP for systems integrated with it; GSA SSO or Contractor recommended automated mechanisms as approved by the GSA CISO and AO*].
(3) Audit Record Review, Analysis, and Reporting | Correlate Audit Record Repositories. Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.
(4) Audit Record Review, Analysis, and Reporting | Central Review and Analysis. Provide and implement the capability to centrally review and analyze audit records from multiple components within the system.
(5) Audit Record Review, Analysis, and Reporting |Integrated Analysis of Audit Records. Integrate analysis of audit records with analysis of [*information system monitoring information; GSA SSO or Contractor recommended data/information collected from other sources as approved by the GSA CISO and AO*] to further enhance the ability to identify inappropriate or unusual activity.
(6) Audit Record Review, Analysis, and Reporting | Correlation With Physical Monitoring. | Correlate information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity.

	Low	Mod	High	LATO	MiSaaS	Federal
AU-6	✓	✓	✓		✓	S
AU-6(1)		✓	✓	✓	✓	S
AU-6(3)		✓	✓			S
AU-6(4)		✓**	✓**			S
AU-6(5)			✓			S

AU-6(6)			✓			S

**-control is applicable at the level listed per GSA OCISO Tailored Moderate Baseline

Guidance for Systems Not Integrated With the ELP

The System Owner/system team are responsible for ensuring system logs are reviewed for unusual activity on a periodic or event driven basis as defined in the system's SSPP as approved by the GISA CISO and AO. Logs must be kept validating such a review has taken place. Systems storing and/or processing PII or sensitive (e.g., financial, CUI) data must review database/application/tool logs. Systems without such data are not required to review database/application/tool logs. Table 6-1 identifies the various layers where logs may be generated.

Table 6-1. System Layers Generating Logs

System Layers
Cloud Service Provider (e.g., AWS)
Operating Systems
Log types requiring review only if PII or sensitive data (e.g., financial, CUI) is in scope: • Databases • Applications • Tools
Security Agent/Device Events

A list of specific anomalous activities for the system should be identified for review and analysis. Examples include:

- Unusual authentication and authorization events;
- Unauthorized data or content manipulation;
- Excessive web application or database activity; and
- Unauthorized or unusual transactions.

System Owners/teams must define their own approach for conducting review of these events and activities, at a frequency or upon event occurrence as defined in the system SSPP. It is not necessary for every team to deploy their own centralized tool such as a SIEM to comply with this guide. Teams can construct an approach which covers audit log review for the components that form their system.

Methods that could be used for audit log review include:

- Creating a roster for audit log review that assigns one team member to this function on a rotating basis;
- Creating a form to certify that audit log review has been conducted based on the specified period or event. For example, a Google Form could be used.

If these reviews indicate a possible compromise the GSA IR Team must be notified and a report prepared concerning the events and rationale identifying it as a potential compromise. System Owners/teams must consider information provided by the ISO Division (e.g., vulnerability emails), Cybersecurity and Infrastructure Security Agency notifications (e.g., Binding Operational Directives/Emergency Directives), or other credible sources to gauge risk to their system and adjust the level of audit review, analysis, and reporting, as warranted.

For enhancement AU-6(1), automated mechanisms as approved by the CISO and AO must be integrated in support of audit record review, analysis, and reporting.

For enhancement AU-6(3), system teams must engage with the ISO Division to determine if achieve situational awareness across the organization.

For enhancement AU-6(4), system teams must implement a capability to centrally review and analyze audit records from multiple components.

For enhancements AU-6(5) and AU-6(6), system teams must integrate analysis of audit records with other monitoring sources, including physical access logs, if applicable, to identify unusual or inappropriate activity.

6.7 AU-7 Audit Record Reduction and Report Generation

Control:

Provide and implement an audit record reduction and report generation capability that:

a. Supports on-demand audit record review, analysis, and reporting requirements and after-the-fact investigations of incidents; and
b. Does not alter the original content or time ordering of audit records.

Control Enhancements:

(1) Audit Record Reduction and Report Generation | Automatic Processing. Provide and implement the capability to process, sort, and search audit records for events of interest based on the following content: [*Source IP, Destination IP, Account Names, Date and Time of Events, Event Type*].

	Low	Mod	High	LATO	MiSaaS	Federal
AU-7		✓	✓			S
AU-7(1)		✓	✓			S

Guidance for Systems Not Integrated with the ELP
System Owners/teams must implement a capability to support on-demand audit review, analysis, reporting, and investigation requirements. The capability must not alter the original content or time ordering of audit records.

For enhancement AU-7 (1), a capability must be able to process, sort, and search logs of interests by source IP, destination IP, account names, time and date of events, and event type.

6.8 AU-8 Time Stamps

Control:

a. Use internal system clocks to generate timestamps for audit records; and
b. Record time stamps for audit records that meet [*GSA SSO or Contractor recommended granularity of time measurement to be approved by the GSA CISO and AO*] and that use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp.

	Low	Mod	High	LATO	MiSaaS	Federal
AU-8	✓	✓	✓			S

Guidance for Systems Not Integrated With ELP
Systems must be configured to:

- Generate timestamps based on internal system clocks;
- Meet the approved granularity of time specified in the system SSPP; and
- Use Coordinated Universal Time or have offset information allowing timestamps to be mapped to it.

6.9 AU-9 Protection of Audit Information

Control:

a. Protect audit information and audit logging tools from unauthorized access, modification, and deletion; and
b. Alert [*the GSA Incident Response Team*] upon detection of unauthorized access, modification, or deletion of audit information.

Control Enhancements:

(2) Protection of Audit Information | Store on Separate Physical Systems or Components. Store audit records [*at least weekly, unless the data is being sent to a secondary system, e.g., the Enterprise Logging Platform,*] in a repository that is part of a physically different system or system component than the system or component being audited.
(3) Protection of Audit Information | Cryptographic Protection. Implement cryptographic mechanisms to protect the integrity of audit information and audit tools.
(4) Protection of Audit Information | Access by Subset of Privileged Users. Authorize access to management of audit logging functionality to only [*privileged users specifically authorized to perform audit management functions (i.e., specified administrators of applications, systems, networks, etc.)*].
Note: ISSOs, ISSMs, and System Owners may be provided read access to audit data; however, they will not have access to audit management functions.

	Low	Mod	High	LATO	MiSaaS	Federal
AU-9	✓	✓	✓			S

AU-9(2)			✓			S
AU-9(3)			✓			S
AU-9(4)		✓	✓			S

Guidance for Systems Not Integrated with the ELP

System owners/teams must restrict access to audit records to authorized personnel as designated by the ISSO/ISSM. Should unauthorized access, modification, or deletion of audit information occur, the GSA IR Team must be informed.

For enhancement AU-9(2), audit logs must be stored (i.e., backed up) to a physically different system than the component the audit logs are from at least weekly. Where possible, backups should be sent to Network Attached Storage or another form of highly redundant storage.

For enhancement AU-9(3), audit logs must be encrypted at rest using encrypted disk volumes. A means of ensuring the integrity of the audit records must be implemented by leveraging mechanisms such as cryptographic checksums.

For AU-9(4), System Owners/teams must protect audit logs and any tools used in support of auditing/logging functions by restricting access to only authorized personnel as designated by the ISSO or ISSM.

6.10 AU-10 Non-Repudiation

Control:

Provide irrefutable evidence that an individual (or process acting on behalf of an individual) has performed [*system specific actions, e.g., such as electronically signing a document, approving a request, or receiving a message*].

	Low	Mod	High	LATO	MiSaaS	Federal
AU-10			✓			S

System Owners are responsible for ensuring system specific actions are not able to be reputed after they have occurred. Configuring system components per the settings established in the Security Engineering (ISE) Division’s Technical Guides and Standards assists in establishing non-repudiation capabilities. Some additional methods supporting non-repudiation include digital signatures and message receipts.

6.11 AU-11 Audit Record Retention

Control:

Retain audit records for [*12 months online and 18 months in cold storage*] to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements.

***Note:** Systems will have until the end of FY24 to allow time for captured logs to grow to the timeframes listed.*

	Low	Mod	High	LATO	MiSaaS	Federal
AU-11	✓	✓	✓		✓	S

Guidance for Systems Not Integrated With the ELP

System Owners/teams must ensure audit records are retained for at least 12 months online and 18 months in cold storage, in compliance with M-21-31. The retention method chosen should support after-the-fact investigation and be compliant with policy and regulatory guidelines. These retention requirements were recently extended from the prior 180-day retention requirement to comply with M-21-31. It will take at least 24 months before GSA systems meet this retention timeframe because newly ingested data has to grow over time. Such records are required to be simultaneously retained at the log source for 60 days.

6.12 AU-12 Audit Record Generation

Control:

a. Provide audit record generation capability for the event types defined in AU-2 a. on [*all components*];
b. Allow [*ISSMs, ISSOs, System Owners, Custodians*] to select the event types that are to be logged by specific components of the system; and
c. Generate audit records for the event types defined in AU-2 c, which includes the audit record content defined in AU-3.

Control Enhancements:

(1) Audit Record Generation | System-Wide and Time-Correlated Audit Trail. Compile audit records from [*all components*] into a system-wide (logical or physical) audit trail that is time correlated to within [*1 minute of UTC*].
(3) Audit Record Generation | Changes by Authorized Individuals. Provide and implement the capability for [*Administrators (Application, System, Network, etc.), ISSOs, ISSMs, System Owners*] to change the logging to be performed on [*all components*] based on [*change management decisions*] within [*minutes*].

	Low	Mod	High	LATO	MiSaaS	Federal
AU-12	✓	✓	✓			S
AU-12(1)			✓			S
AU-12(3)			✓			S

GSA systems must be able to generate audit records for the auditable events specified in AU-2a with the content in AU-3 for all system components. System Owners, Custodians, ISSOs, and ISSMs must collaborate on which specific events are to be audited by specific components.

Platforms, including the cloud service provider layer where applicable, must coordinate with systems and applications they support to ensure that components at the platform level meet the AU-12 requirement.

Table 6-2 contains of system components and the logs associated with them that are capable of generating audit records.

Table 6-2. Examples of System Component Logs

System Components	Logs
Cloud Service Provider (e.g., AWS, Azure, etc.)	• Cloud Trail • CloudWatch logs (if used for security alerting) • VPC Flow logs
Operating Systems	• Linux/UNIX • Windows
Databases	• Oracle • MySQL • PostgreSQL • Others
Applications	• Apache • Drupal • WordPress • Solr • Security agents • Others
Tools	• Jenkins • Tableau • Others
Security Agent/Device Events	• Bit9 • ClamAV • Others

For enhancement AU-12(1), audit records must be time correlated to within 1 minute of UTC.

For enhancement AU-12(3), on a case-by-case basis, coordination between the ISO and ISE Divisions, System Owners, and ISSOs/ISSMs can identify recommended changes to system auditing and, following the system's change management process, system personnel can adjust auditing as necessary.

7 Vendor/Contractor Systems

7.1 AU-1 Audit and Accountability Policy and Procedures

Control:

a. Develop, document, and disseminate to [*personnel with IT security responsibilities as defined in GSA Order CIO 2100.1*]:
   1. [*Organization-level*] audit and accountability policy that:
      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
   2. Procedures to facilitate the implementation of the audit and accountability policy and the associated audit and accessibility controls;

b. Designate an [*CISO*] to manage the development, documentation, and dissemination of the audit and accessibility policy and procedures; and

c. Review and update the current audit and accessibility:
   1. Policy [*annually, as part of CIO 2100.1 update*] and following [*changes to Federal or GSA policies, requirements, or guidance*]; and
   2. Procedures [*at least every three (3) years*] and following [*changes to Federal or GSA policies, requirements, or guidance*].

	Low	Mod	High	LATO	MiSaaS	Contractor
AU-1	✓	✓	✓			H

Common Control Implementation
GSA's audit and accountability policy is defined in the GSA IT Security Policy, CIO 2100.1, which addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance regarding audit and accountability for GSA systems. This policy is maintained to be consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines by updating the policy via Changes, Instructional Letters, or the annual update as applicable. This policy is disseminated GSA-wide via directive library webpages on GSA.gov and GSA's InSite websites.

GSA's audit and accountability procedures are documented in GSA IT Security Procedural Guide: CIO-IT Security-01-08, Audit and Accountability (AU) [this guide]. The procedures facilitate the implementation of the audit and accountability policy and associated controls. This guide is disseminated GSA-wide via IT Security Procedural Guides webpages on GSA.gov and GSA's InSite websites.

Per 2100.1, the CISO is responsible for managing the development and publishing of all security policies and IT security procedural guides. The GSA OCISO is responsible for reviewing and updating CIO 2100.1 annually. The GSA OCISO is responsible for reviewing and updating CIO-IT Security-01-08 every three years and following changes to Federal or GSA policies, requirements, or guidance.

GSA Service and Staff Officers (SSOs) or system owners may augment the access control policies and procedures included in 2100.1 and CIO-IT Security-01-08 to address additional organizational or system-specific configuration management requirements. Any such policies and procedures must establish timeframes for updates.

Vendor/Contractor Systems

Vendors/contractors may defer to the GSA policy and guide or implement their own audit and accountability policies and procedures which comply with GSA's requirements with the approval of the GSA CISO and AO.

7.2 AU-2 Event Logging

Control:

f. Identify the types of events that the system is capable of logging in support of the audit function: [
    (1) *successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events;*
    (2) *Web applications should log all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes;*
    (3) *for technologies with limited auditing features, the capabilities will be recommended by the GSA SSO or Contractor, based on an industry source such as vendor guidance or Center for Internet Security benchmark, and approved by the GSA CISO and AO*];

g. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged;

h. Specify the following event types for logging within the system: [
    (1) *audit configuration requirements as documented in applicable GSA IT Security Technical Guides and Standards (i.e., hardening and technology implementation guides)*
    (2) *for web applications see GSA IT Security Procedural Guide 07-35, Section 2.8.10, What to Log*
    (3) *for technologies where a Technical Guide and Standard does not exist, events from an industry source such as vendor guidance or Center for Internet Security benchmark, recommended by the GSA SSO or Contractor and approved by the GSA CISO and AO*];

i. Provide a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and

j. Review and update the event types selected for logging [*annually or whenever there is a change in the system's threat environment as communicated by the GSA SSO AO or the GSA OCISO*].

	Low	Mod	High	LATO	MiSaaS	Contractor
AU-2	✓	✓	✓	✓	✓	S

Vendor/Contractor Systems

For Vendor/Contractor systems, the GSA ISSO must coordinate with the System Owner/team to ensure the AU-2 controls are met. Actions required include:

- ensuring coordination of event logging with other entities (e.g., GSA security personnel, vendor/contractor security personnel) to inform event selection;
- coordinating the configuration of logging/auditing functions to log events based on GSA's hardening guides and web application security guide or vendor settings with the approval of the CISO and AO, and establishing approved logging for technologies where no GSA or vendor/contractor guidance exists;
- ensuring the rationale for why the selected events are adequate to support investigations is documented; and
- ensuring the annual review and update, if applicable, of selected events as part of the SSPP review and update, or if the system's threat environment changes.

Regarding the selection of events to be audited, vendors/contractors may align with hardening guides and associated benchmarks that are available on the IT Security Technical Guides and Standards webpage, or use their own or other industry best practices with the approval of the CISO and AO.

7.3 AU-3 Content of Audit Records

Control:

Ensure that audit records contain information that establishes the following:

a. What type of event occurred;
b. When the event occurred;
c. Where the event occurred;
d. Source of the event;
e. Outcome of the event; and
f. Identity of any individuals, subjects, or objects/entities associated with the event.

Control Enhancements:

(1) Content of Audit Records | Additional Audit Information. Generate audit records containing the following additional information: [

i. *Session, connection, transaction, or activity duration;*
ii. *For client-server transactions, the number of bytes received, and bytes sent. This gives bidirectional transfer information that can be helpful during an investigation or inquiry;*
iii. *For client-server transactions, unique metadata or properties about the client initiating the transaction. This could include properties such as an IP address, user name, session identifier, or browser characteristics (e.g., a 'User-Agent' string).*
iv. *Details regarding the event 'type': the type of method (for HTTP: GET/POST/HEAD, etc.) or action (Database INSERT, UPDATE, DELETE);*
v. *Characteristics that describe or identify the object or resource being acted upon; and*
vi. *Additional informational messages to diagnose or identify the event].*

(3) Content of Audit Records | Limit Personally Identifiable Information Elements. Limit personal identifiable information contained in audit records to the following elements identified in the privacy risk assessment: [*no PII to be included in audit records*].

(4)	Low	Mod	High	LATO	MiSaaS	Contractor
AU-3	✓	✓	✓		✓	S
AU-3(1)		✓	✓			S
AU-3(3)		✓^	✓^			S

^-control is applicable if PII is stored, processed, or transmitted

Vendor/Contractor Systems
The System Owner/team is responsible for ensuring the required content of audit records is captured.

For enhancement AU-3(1), the System Owner/team is responsible for ensuring that the system is configured to properly generate the additional information required by GSA's parameter.

For enhancement AU-3(3), the System Owner/team are responsible for ensuring PII data and sensitive data, such as financial data, are not stored in logs.

7.4 AU-4 Audit Log Storage Capacity

Control:

Allocate audit log storage capacity to accommodate [*GSA policies and guidance: audit log sizes are documented in applicable GSA IT Security Technical Guides and Standards (i.e., hardening and technology implementation guides) available on the IT Security Technical Guides and Standards webpage*].

	Low	Mod	High	LATO	MiSaaS	Contractor
AU-4	✓	✓	✓			S

Vendor/Contractor Systems
Logs should be stored by the system team either on the host itself or in a storage repository (i.e., the team has access to options such as network-attached storage or S3). The storage type used must be durable to avoid loss of audit logs. Per control AU-11, logs must be retained for a minimum of 12 months online and 18 months in cold storage by the end of FY24. This timeline allows systems to grow audit logs since this is a recent change from the previous requirement of 6 months for log retention.

7.5 AU-5 Response to Audit Logging Process Failures

Control:

a. Alert [*the GSA Enterprise Security Operation Center ~~ISO Division~~ via the ELP for systems integrated with it; Administrators (Application, System, Network, etc.) for systems not* *integrated with the ELP*] within [*GSA SSO or Contractor recommended time period as approved by the GSA CISO and AO*] in the event of an audit logging process failure; and

b. Take the following additional actions: [*shut down information system, overwrite oldest audit records, or stop generating audit records*].

Control Enhancements:

(1) Response to Audit Logging Process Failures | Storage Capacity Warning. Provide a warning to [*Administrators (Application, System, Network, etc.)*] within [*GSA SSO or Contractor recommended time period as approved by the GSA CISO and AO*] when allocated audit log storage volume reaches [*GSA SSO or Contractor recommended percentage as approved by the GSA CISO and AO*] of repository maximum audit record storage capacity.

(2) Response to Audit Logging Process Failures | Real-Time Alerts. Provide an alert within [*GSA SSO or Contractor recommended time period as approved by the GISA CISO and AO*] to [*the GSA ISO Division via the ELP for systems integrated with the ELP, Administrators (Application, System, Network, etc.) for systems not integrated with the ELP*] when the following audit failure events occur: [*GSA SSO or Contractor recommended audit failure events requiring real-time alerts as approved by the GSA CISO and AO*].

	Low	Mod	High	LATO	MiSaaS	Contractor
AU-5	✓	✓	✓			S
AU-5(1)			✓			S
AU-5(2)			✓			S

Vendor/Contractor Systems

The System Owner/team must configure alerts to be sent within the system's specified time period to the system's specified personnel in the event of audit log process failures and systems will have to take one of the actions listed in the AU-5, part b, parameter upon audit processing failure.

For enhancement AU-5(1), systems will have to configure warnings for the roles/personnel within the system's specified timeframe, when the system's specified percentage of capacity for log storage is reached.

For enhancement AU-5(2), systems will have to configure alerts within the system's specified time period to the system's specified personnel when the system's specified alerts occur.

The GSA CISO and AO must approve all warning and alert parameters.

7.6 AU-6 Audit Record Review, Analysis, and Reporting

Control:

a. Review and analyze system audit records [*Systems integrated with the ELP where automated analysis and correlations is performed: on business days; otherwise on a periodic or event driven basis (periodicity or events driving reviews are recommended by the GSA SSO or Contractor and approved by the GSA CISO and AO)*] for indications of [*GSA SSO or Contractor recommended inappropriate or unusual activity as approved by the GSA CISO and AO*] and the potential impact of the inappropriate or unusual activity;
b. Report findings to [*ISSM, ISSO, System Owner, Custodian, as designated and approved by the GSA CISO and AO, via a dashboard when events are forwarded to the ELP, otherwise via an alternative automated or manual reporting mechanisms*]; and
c. Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.

Control Enhancements:

(1) Audit Record Review, Analysis, and Reporting | Automated Process Integration. Integrate audit record review, analysis, and reporting processes using [*the GSA ELP for systems integrated with it; GSA SSO or Contractor recommended automated mechanisms as approved by the GSA CISO and AO*].
(3) Audit Record Review, Analysis, and Reporting | Correlate Audit Record Repositories. Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.
(4) Audit Record Review, Analysis, and Reporting | Central Review and Analysis. Provide and implement the capability to centrally review and analyze audit records from multiple components within the system.
(5) Audit Record Review, Analysis, and Reporting |Integrated Analysis of Audit Records. Integrate analysis of audit records with analysis of [*information system monitoring information; GSA SSO or Contractor recommended data/information collected from other sources as approved by the GSA CISO and AO*] to further enhance the ability to identify inappropriate or unusual activity.
(6) Audit Record Review, Analysis, and Reporting | Correlation With Physical Monitoring. | Correlate information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity.

	Low	Mod	High	LATO	MiSaaS	Contractor
AU-6	✓	✓	✓		✓	S
AU-6(1)		✓	✓	✓	✓	S
AU-6(3)		✓	✓			S
AU-6(4)		✓**	✓**			S
AU-6(5)			✓			S
AU-6(6)			✓			S

**-control is applicable at the level listed per GSA OCISO Tailored Moderate Baseline

Vendor/Contractor Systems

The System Owner/system team are responsible for ensuring system logs are reviewed for unusual activity on a periodic or event driven basis as defined in the system's SSPP as approved by the GISA CISO and AO. Logs must be kept validating such a review has taken place. Systems storing and/or processing PII or sensitive (e.g., financial, CUI) data must review database/application/tool logs. Systems without such data are not required to review database/application/tool logs. Table 7-1 identifies the various layers where logs may be generated.

Table 7-1. System Layers Generating Logs

System Layers
Cloud Service Provider (e.g., AWS)
Operating Systems
Log types requiring review only if PII or sensitive data (e.g., financial, CUI) is in scope: • Databases • Applications • Tools
Security Agent/Device Events

A list of specific anomalous activities for the system should be identified for review and analysis. Examples include:

- Unusual authentication and authorization events;
- Unauthorized data or content manipulation;
- Excessive web application or database activity; and
- Unauthorized or unusual transactions.

System Owners/teams must define their own approach for conducting review of these events and activities, at a frequency or upon event occurrence as defined in the system SSPP. It is not necessary for every team to deploy their own centralized tool such as a SIEM to comply with this guide. Teams can construct an approach which covers audit log review for the components that form their system.

Methods that could be used for audit log review include:

- Creating a roster for audit log review that assigns one team member to this function on a rotating basis;
- Creating a form to certify that audit log review has been conducted based on the specified period or event. For example, a Google Form could be used.

If these reviews indicate a possible compromise the GSA IR Team must be notified and a report prepared concerning the events and rationale for identifying it as a potential compromise. System Owners/teams must consider information provided by the vendor/contractor's security team (e.g., vulnerability notifications), Cybersecurity and Infrastructure Security Agency notifications (e.g., Binding Operational Directives/Emergency Directives), or other credible sources to gauge risk to their system and adjust the level of audit review, analysis, and reporting, as warranted.

For enhancement AU-6(1), automated mechanisms as approved by the CISO and AO must be integrated in support of audit record review, analysis, and reporting.

For enhancement AU-6(3), system teams must engage with the vendor/contractor's security team to achieve situational awareness across the organization.

For enhancement AU-6(4), system teams must implement a capability to centrally review and analyze audit records from multiple components.

For enhancements AU-6(5) and AU-6(6), system teams must integrate analysis of audit records with other monitoring sources, including physical access logs, if applicable, to identify unusual or inappropriate activity.

7.7 AU-7 Audit Record Reduction and Report Generation

Control:

Provide and implement an audit record reduction and report generation capability that:

a. Supports on-demand audit record review, analysis, and reporting requirements and after-the-fact investigations of incidents; and
b. Does not alter the original content or time ordering of audit records.

Control Enhancements:

(1) Audit Record Reduction and Report Generation | Automatic Processing. Provide and implement the capability to process, sort, and search audit records for events of interest based on the following content: [*Source IP, Destination IP, Account Names, Date and Time of Events, Event Type*].

	Low	Mod	High	LATO	MiSaaS	Contractor
AU-7		✓	✓			S
AU-7(1)		✓	✓			S

Vendor/Contractor Systems

System Owners/teams must implement a capability to support on-demand audit review, analysis, reporting, and investigation requirements. The capability must not alter the original content or time ordering of audit records.

For enhancement AU-7 (1), a capability must be able to process, sort, and search logs of interests by source IP, destination IP, account names, time and date of events, and event type.

7.8 AU-8 Time Stamps

Control:

a. Use internal system clocks to generate timestamps for audit records; and
b. Record time stamps for audit records that meet [*GSA SSO or Contractor recommended granularity of time measurement to be approved by the GSA CISO and AO*] and that use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp.

	Low	Mod	High	LATO	MiSaaS	Contractor
AU-8	✓	✓	✓			S

Vendor/Contractor Systems
Systems must be configured to:

- Generate timestamps based on internal system clocks;
- Meet the approved granularity of time specified in the system SSPP; and
- Use Coordinated Universal Time or have offset information allowing timestamps to be mapped to it.

7.9 AU-9 Protection of Audit Information

Control:

a. Protect audit information and audit logging tools from unauthorized access, modification, and deletion; and
b. Alert [*the GSA Incident Response Team*] upon detection of unauthorized access, modification, or deletion of audit information.

Control Enhancements:

(2) Protection of Audit Information | Store on Separate Physical Systems or Components. Store audit records [*at least weekly, unless the data is being sent to a secondary system, e.g., the Enterprise Logging Platform,*] in a repository that is part of a physically different system or system component than the system or component being audited.
(3) Protection of Audit Information | Cryptographic Protection. Implement cryptographic mechanisms to protect the integrity of audit information and audit tools.
(4) Protection of Audit Information | Access by Subset of Privileged Users. Authorize access to management of audit logging functionality to only [*privileged users specifically authorized to perform audit management functions (i.e., specified administrators of applications, systems, networks, etc.)*].

Note: ISSOs, ISSMs, and System Owners may be provided read access to audit data; however, they will not have access to audit management functions.

	Low	Mod	High	LATO	MiSaaS	Contractor
AU-9	✓	✓	✓			S

AU-9(2)			✓			S
AU-9(3)			✓			S
AU-9(4)		✓	✓			S

Vendor/Contractor Systems
System owners/teams must restrict access to audit records to authorized personnel as designated by the ISSO/ISSM. Should unauthorized access, modification, or deletion of audit information occur, the GSA IR Team must be informed.

For enhancement AU-9(2), audit logs must be stored (i.e., backed up) to a physically different system than the component the audit logs are from at least weekly. Where possible, backups should be sent to Network Attached Storage or another form of highly redundant storage.

For enhancement AU-9(3), audit logs must be encrypted at rest using encrypted disk volumes. A means of ensuring the integrity of the audit records must be implemented by leveraging mechanisms such as cryptographic checksums.

For AU-9(4), System Owners/teams must protect audit logs and any tools used in support of auditing/logging functions by restricting access to only authorized personnel as designated by the GSA ISSO or ISSM.

7.10 AU-10 Non-Repudiation

Control:

Provide irrefutable evidence that an individual (or process acting on behalf of an individual) has performed [*system specific actions, e.g., such as electronically signing a document, approving a request, or receiving a message*].

Platform/system/application System Owners are responsible for ensuring system specific actions are not able to be reputed after they have occurred. Configuring platforms/systems/applications per the settings established in the Security Engineering (ISE) Division's Technical Guides and Standards assists in establishing non-repudiation capabilities. Some additional methods supporting non-repudiation include digital signatures and message receipts.

	Low	Mod	High	LATO	MiSaaS	Contractor
AU-10			✓			S

Vendor/Contractor Systems
Vendors/contractors are required to comply with the control statement.

7.11 AU-11 Audit Record Retention

Control:

Retain audit records for [*12 months online and 18 months in cold storage*] to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements.

Note: *Systems will have until the end of FY24 to allow time for captured logs to grow to the timeframes listed.*

	Low	Mod	High	LATO	MiSaaS	Contractor
AU-11	✓	✓	✓		✓	S

Vendor/Contractor Systems
System Owners/teams must ensure audit records are retained for at least 12 months online and 18 months in cold storage, in compliance with M-21-31. The retention method chosen should support after-the-fact investigation and be compliant with policy and regulatory guidelines. These retention requirements were recently extended from the prior 180-day retention requirement to comply with M-21-31. It will take at least 24 months before GSA systems meet this retention timeframe because newly ingested data has to grow over time. Such records should be simultaneously retained at the log source for 60 days.

7.12 AU-12 Audit Record Generation

Control:

a. Provide audit record generation capability for the event types defined in AU-2 a. on [*all components*];
b. Allow [*ISSMs, ISSOs, System Owners, Custodians*] to select the event types that are to be logged by specific components of the system; and
c. Generate audit records for the event types defined in AU-2 c, which includes the audit record content defined in AU-3.

Control Enhancements:

(1) Audit Record Generation | System-Wide and Time-Correlated Audit Trail. Compile audit records from [*all components*] into a system-wide (logical or physical) audit trail that is time correlated to within [*1 minute of UTC*].
(3) Audit Record Generation | Changes by Authorized Individuals. Provide and implement the capability for [*Administrators (Application, System, Network, etc.), ISSOs, ISSMs, System Owners*] to change the logging to be performed on [*all components*] based on [*change management decisions*] within [*minutes*].

	Low	Mod	High	LATO	MiSaaS	Contractor
AU-12	✓	✓	✓			S
AU-12(1)			✓			S
AU-12(3)			✓			S

Vendor/Contractor Systems

Vendor/contractor systems must be able to generate audit records for the auditable events specified in AU-2a with the content in AU-3 for all system components. System Owners, Custodians, ISSOs, and ISSMs must collaborate on which specific events are to be audited by specific components.

Appendix A: CSF Categories/Subcategories

The CSF focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes. The core of the CSF consists of five concurrent and continuous Functions—Identify (ID), Protect (PR), Detect (DE), Respond (RS), and Recover (RC). The CSF complements, and does not replace, an organization's risk management process and cybersecurity program. GSA uses NIST's Risk Management Framework (RMF) from NIST SP 800-37, Revision 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. Table A-1 lists the Categories and Subcategories from the CSF that are identified as related to the implementation of policies, procedures, and processes implementing the NIST SP 800-53 AU family. GSA CIO Order 2100.1 and this procedural guide provide GSA's policies and procedural guidance regarding access control for GSA IT systems and AU controls.

Table A-1: CSF Categories/Subcategories

CSF Category	CSF Subcategories
Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	**ID.GV-1:** Organizational cybersecurity policy is established and communicated *(AU-1)* **ID.GV-3:** Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed *(AU-1)*
Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	**ID.SC-4:** Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations *(AU-6)*
Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-4:** Adequate capacity to ensure availability is maintained *(AU-4)*
Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy *(AU-1, AU-2, AU-3, AU-6, AU-7, AU-12)*
Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.	**DE.AE-2:** Detected events are analyzed to understand attack targets and methods *(AU-6)* **DE.AE-3:** Event data are collected and correlated from multiple sources and sensors *(AU-6)*
Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify.	**DE.CM-1:** The network is monitored to detect potential cybersecurity events *(AU-12)* **DE.CM-3:** Personnel activity is monitored to detect potential cybersecurity events *(AU-12)*

CSF Category	CSF Subcategories
	DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed *(AU-12)*
Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	**DE.DP-4:** Event detection information is communicated *(AU-6)*
Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g., external support from law enforcement agencies).	**RS.CO-2:** Incidents are reported consistent with established criteria *(AU-6)*
Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated *(AU-6)* **RS.AN-3:** Forensics are performed *(AU-7)*

Appendix B: CIO 2100.1 Policy Statements on Audit and Accountability

The following extracts from GSA Order CIO 2100.1 contain information related to audit and accountability.

Chapter 4: Policy for Protection states:

6. Protective Technology.

   a. The requirements for security auditing/logging capabilities and their review must be implemented on GSA systems IAW GSA CIO-IT Security-01-08, Audit and Accountability.

   c. Auditing of actions regarding PII stored on network drives and/or application databases must be captured (e.g., type of action, date/time, user, source of action, outcome of action)

Chapter 5: Policy for Detect Function states:

1. Anomalies and Events.

   c. The OCISO will regularly review/analyze data provided with the ELP for indications of inappropriate or unusual activity. Suspicious activity or suspected violations must be investigated. Any findings must be reported to appropriate officials IAW GSA CIO-IT Security-01-02.

   d. Information systems must produce audit/log records containing sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.

   e. The OCISO ELP will be used for the collection and correlation from GSA systems/sensors.

2. Security Continuous Monitoring.

   d. Monitoring procedures must include specific steps to be taken and protocol to be applied when reviewing audit/log data.

   e. The OCISO must be informed in the event of an audit processing failure, and system personnel must take one of the following additional actions: shut down the information system, overwrite the oldest audit records, or stop generating audit records.

Appendix C: References

Federal Laws, Standards, Regulations, and Publications:

- EO 13800, "Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure"
- FIPS PUB 199, "Standards for Security Categorization of Federal Information and Information Systems"
- NIST Cybersecurity Framework, "Framework for Improving Critical Infrastructure Cybersecurity"
- 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"
- NIST SP 800-161, Revision 1, "Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations"
- OMB M-21-31, "Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents"
- Public Law 113-283, "Federal Information Security Modernization Act of 2014"

GSA Policies, Procedures, Guidance:

The GSA policy listed below is available on the GSA.gov Directives Library page.

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

The GSA CIO-IT Security Procedural Guides listed below are available on the GSA.gov IT Security Procedural Guides page with the exception of CIO-IT Security-18-90 which is restricted. It is available on the internal GSA InSite IT Security Procedural Guides page.

- 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-18-90: Information Security Program Plan (ISPP)

Appendix D: Roles and Responsibilities

The roles and responsibilities provided in this appendix have been extracted or paraphrased from GSA Order CIO 2100.1 or summarized from GSA and Federal guidance. Complete roles and responsibilities for agency management officials and roles with significant IT Security responsibilities are defined in GSA CIO Order 2100.1.

Authorizing Officials (AOs)

Responsibilities include the following:

- Ensuring that GSA information systems under their purview have implemented the required AU controls in accordance with GSA and Federal policies and requirements.
- Identifying the level of acceptable risk for an information system and determining whether an acceptable level of risk has been obtained, including risks associated with AU controls.
- Ensuring all information systems, applications, or sets of common controls under their purview have a current ATO issued IAW GSA CIO-IT Security-06-30.
- Ensuring a plan of action and milestones (POA&M) item is established and managed to address AU controls that are not fully implemented.

Information Systems Security Officers (ISSOs)

Responsibilities include the following:

- Ensuring necessary AU security controls are in place and operating as intended.
- Coordinating with ISSMs to establish and manage auditing and monitoring procedures (e.g., reviewing and coordinating the reporting of security alerts, performance of audit log reviews, supporting the use of auditing/logging as part of security incident investigations and reports, etc.).
- Reviewing audit/log reports for systems integrated with the GSA Enterprise Logging Platform (ELP) for potential security issues.
- Verifying systems not integrated with the GSA ELP/audit logging tool perform similar reviews to identify potential security issues.
- Working with the System Owner and ISSM to develop, implement, and manage POA&Ms regarding AU controls for their respective systems IAW GSA CIO-IT Security-09-44.
- Working with System Owners to ensure the appropriate level of auditing and logging data is enabled and generated to support monitoring activities and supports GSA's plan to comply with OMB M-21-31 active and cold data storage time frames.
- Working with Systems Owners to audit user activity for indications of fraud, misconduct, or other irregularities.
- Working with System Owners to document all phases of monitoring activity including monitoring procedures, response processes, and steps performed when reviewing user activity.

Information Systems Security Managers (ISSMs)

Responsibilities include the following:

- Assisting ISSOs to ensure the necessary AU security controls are in place and operating as intended.
- Coordinating with ISSOs to establish and manage auditing and monitoring procedures (e.g., reviewing and coordinating the reporting of security alerts, performance of audit log reviews, supporting the use of auditing/logging as part of security incident investigations and reports, etc.).
- Working with the ISSO and System Owner to develop, implement, and manage POA&Ms regarding AU controls for their respective systems IAW GSA CIO-IT Security-09-44.

System Owners

Responsibilities include the following:

- Ensuring necessary AU security controls are in place and operating as intended.
- Working with ELP personnel to ensure audit record formats for their systems can be processed by the ELP.
- Working with Data Owners to ensure the appropriate level of auditing and logging data is enabled and generated to support monitoring activities and archived for a period of not less than 180 days.
- Working with Data Owners to audit user activity for indications of fraud, misconduct, or other irregularities.
- Working with Data Owners to document all phases of monitoring activity including monitoring procedures, response processes, and steps performed when reviewing user activity.
- Working with the ISSO and ISSM to develop, implement, and manage POA&Ms regarding AU controls for their respective systems IAW GSA CIO-IT Security-09-44.
- Assigning system personnel to review any logs not forwarded to the ELP.

Data Owners

Responsibilities include the following:

- Coordinating with IT security personnel including the ISSM, ISSO, and System Owners to ensure implementation of system and data controls, including AU controls.
- Working with the system owner to ensure the appropriate level of auditing and logging data is enabled and generated to support monitoring activities and supports GSA’s plan to comply with OMB M-21-31 active and cold data storage time frames.
- Working with the System Owner to audit user activity for indications of fraud, misconduct, or other irregularities.
- Working with the System Owner to document all phases of monitoring activity including monitoring procedures, response processes, and steps performed when reviewing user activity.

System/Network Administrators

Responsibilities include the following:

- Ensuring the appropriate AU security requirements are implemented consistent with GSA IT security policies and hardening guidelines.
- Performing audit/log reviews for systems not integrated with the GSA ELP to identify potential security issues as specified in the system's system security and privacy plan (SSPP).

ELP Personnel

Responsibilities include the following:

- Working with the ISSM, ISSO, System Owner, and System Administrators to ensure audit/log data is enabled and configured to send logs to the ELP.
- Investigating with the ISSM, ISSO, System Owner, and System Administrators when issues are identified regarding audit/log data being sent to the ELP.
- Coordinating with the ISSM, ISSO, System Owner, and System Administrators regarding alerts, responses to audit/log failure, and reviews of audit/log data.