

# **Information Technology (IT) Audit and Accountability (AU) Standard**

**January 26, 2024**

**U.S. Department of Education (ED)  
Office of the Chief Information Officer (OCIO)  
Information Assurance Services (IAS)**



Questions about the policies outlined in this document should be directed to Information Assurance Services (IAS) at [IAS\\_Governance@ed.gov](mailto:IAS_Governance@ed.gov).

## **APPROVAL**

---

**Steven Hernandez**  
**Director, IAS/Chief Information Security Officer (CISO)**

## Revision History

The table below identifies all changes that have been incorporated into this document.

Version	Date	Summary of Changes
1.0	12/24/2021	Initial draft of new standard which combines NIST SP 800-53, Revision 5 controls, including ED specific control parameter values, with existing policy standards and requirements from OMB M-21-31.
1.1	1/18/2022	Update to incorporate feedback from Information Assurance Services (IAS), Governance, Risk and Policy (GRP) Team.
1.2	1/31/2022	Update to incorporate feedback from IAS; address new security measures required by Executive Order (EO) 14028, including Office of Management and Budget (OMB) regulations and memoranda and updated NIST guidance issued to comply with the EO.
1.3	1/26/2023	Annual Review. Correct AU-7 by removing requirement for low baseline. Add “statutory” to AU-11. Updated AU-12(3) to include frequency CPV
1.4	2/7/2023	Updated AU-12(3) to include frequency CPV. (not sure why removed from update) Remove Erroneous “L” from AU-7(1) control Heading
5.5	1/26/2024	Aligned document major version number to align with NIST SP 800-53 revision number. Clean up formatting and numbering throughout and update broken links. Section 2, Standards was updated to include the description of incorporating organizationally defined parameters (ODP) for controls that may be necessary from external control overlays (e.g., High Value Assets [HVA]). Inserted references to NIST SP 800-53B tailoring guidance. Updated Section 4, Acronyms as appropriate. Updated language in controls AU-01 and AU-06. Added controls AU-06(04), AU-06(07), AU-06(09), AU-09(05), AU-09(06), AU-16, AU-16(01), and AU-16(02). Added “leading zeros” to control identifiers in alignment with patch release of NIST SP 800-53 (Release 5.1.1) to applicable controls, enhancements, and overlays.

# Table of Contents

- 1 INTRODUCTION ..... 1
  - 1.1 Purpose..... 1
  - 1.2 Scope..... 1
- 2 STANDARDS..... 2
  - 2.1 AU-01 Policy and Procedures (P, L, M, H) ..... 2
  - 2.2 AU-02 Event Logging (P, L, M, H and Control Overlay) ..... 3
  - 2.3 AU-03 Content of Audit Records (L, M, H) ..... 4
  - 2.4 AU-04 Audit Log Storage Capacity (L, M, H, and Control Overlay) ..... 5
  - 2.5 AU-05 Response to Audit Logging Process Failures (L, M, H) ..... 5
  - 2.6 AU-06 Audit Record Review, Analysis, and Reporting (L, M, H and Control Overlay)..... 5
  - 2.7 AU-07 Audit Recording Reduction and Report Generation (M, H) ..... 7
  - 2.8 AU-08 Time Stamps (L, M, H)..... 7
  - 2.9 AU-09 Protection of Audit Information (L, M, H) ..... 7
  - 2.10 AU-10 Non-repudiation (H)..... 8
  - 2.11 AU-11 Audit Record Retention (P, L, M, H)..... 8
  - 2.12 AU-12 Audit Record Generation (L, M, H)..... 8
  - 2.13 AU-16 Cross-Organizational Audit Logging..... 9
- 3 RISK ACCEPTANCE/POLICY EXCEPTIONS ..... 10
- 4 ACRONYMS ..... 11
- APPENDIX A - BASELINE CONTROL PARAMETER SUMMARY ..... 13

# 1 INTRODUCTION

This governance document establishes U.S. Department of Education (ED or Department) information technology (IT) system audit and accountability standards necessary to improve the efficiency of operation or security of Department information systems and comply with Federal laws, regulations, Executive Orders (EO), Emergency Orders, Binding Operational Directives (BOD), and Department Administrative Communications System Directives (ACSD) and Handbooks. In doing so, these standards supersede any prior governance documentation establishing such standards.

## 1.1 Purpose

The Federal Information Security Modernization Act (FISMA)<sup>1</sup> and implementing governance Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource*<sup>2</sup>, requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source, and services that are either fully or partially provided, including agency-hosted, outsourced, and cloud-based solutions. Federal Information Processing Standards (FIPS) Publication (PUB) 200, *Minimum Security Requirements for Federal Information and Information Systems*<sup>3</sup>, mandates the use of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Security and Privacy Controls for Information Systems and Organizations*<sup>4</sup>, as amended, as baseline information system controls.

## 1.2 Scope

These standards apply to all information and information systems that support the operations and assets of the Department, including those provided or managed by another agency, contractor, or other source, as well as services that are either fully or partially provided, including Department-hosted, outsourced, and cloud-based solutions. Principal Offices, employees, contractors, external service providers and system users are required to comply with these system audit and accountability standards control standards.

---

<sup>1</sup> Public Law 113-283-Dec. 18, 2014, <https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf>

<sup>2</sup> Office of Management and Budget (OMB) Circular A-130, [https://www.whitehouse.gov/wp-content/uploads/legacy\\_drupal\\_files/omb/circulars/A130/a130revised.pdf](https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf)

<sup>3</sup> FIPS 200, <https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.200.pdf>

<sup>4</sup> NIST SP 800-53, <https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final>

## 2 STANDARDS

The Department standards for IT system audit and accountability controls are organized to follow the order in which controls are presented in the current version of NIST SP 800-53. To define a control baseline for Department information systems, a FIPS PUB 199 categorization level (e.g., Low [L], Moderate [M] and High [H]) is assigned to each requirement. This designator indicates a requirement applies to information systems categorized at that FIPS PUB 199 impact-level. Designators are also used to indicate when NIST SP 800-53 Privacy (P) baseline controls are required. To manage risk to within the Department's risk tolerance and appetite, control overlays are provided when the Department requires implementation of control(s) that are not required by the FIPS PUB 199 impact-level or privacy baseline.

In addition to the controls required by this standard, High Value Assets (HVAs) must implement and comply with the current version of the HVA Control Overlay issued and maintained by the Department of Homeland Security (DHS), Cybersecurity & Infrastructure Security Agency (CISA). Systems that process federal tax information (FTI) must implement and comply with the Internal Revenue Service (IRS) Publication 1075<sup>5</sup>, *Tax Information Security Guidelines for Federal, State and Local Agencies: Safeguards for Protecting Federal Tax Returns and Return Information*. Systems that are Federal Risk and Authorization Management Program (FedRAMP) authorized must implement and comply with the FedRAMP identified baselines<sup>6</sup>.

Throughout the standard, there are controls captured that have not been scoped to any specific security or privacy baseline. This is intentional as all controls for identified external overlays and baselines (e.g., FedRAMP, IRS, HVA), that may apply to systems within the Department, have been incorporated into the standard. This ensures the organization defined parameters (ODPs) for controls within the Department have been clearly defined in a consistent manner.

This standard directly supports the Department's integration of the NIST Cybersecurity Framework (CSF) and NIST Privacy Framework (PF) by using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the Department's risk management processes. Refer to *APPENDIX A - BASELINE CONTROL PARAMETER SUMMARY* for a summary of controls by baseline and corresponding NIST CSF and NIST PF categories and subcategories.

### 2.1 AU-01 Policy and Procedures (P, L, M, H)

The Department shall develop, document, and disseminate to all ED employees, contractors, and users authorized to access to ED information systems, or systems operated or maintained on behalf of ED, or ED information as defined in ACSD-OCIO-004<sup>7</sup>, Cybersecurity Policy, ACSD-OCIO-

---

<sup>5</sup> IRS Publication 1075 <https://www.irs.gov/pub/irs-pdf/p1075.pdf>

<sup>6</sup> FedRAMP baselines <https://www.fedramp.gov/baselines/>

<sup>7</sup> Also known as OCIO: 3-112.

011<sup>8</sup>, *Software Asset Management Acquisition Policy*, ACSD-OFO-006<sup>9</sup>, *Acquisition Planning, Acquisition Procedures Manual*, and *Security and Privacy Requirements for IT Procurements*, a Department-level system and services acquisition policy (e.g., this document) 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;
- c. authorizes the Department Chief Information Security Officer (CISO) and Department Chief Information Officer (CIO) to issue subordinate standards, procedures, and memos, with the same authority and enforcement as ACSD-OCIO-004, *Cybersecurity Policy*.

The Department CISO in conjunction with the Senior Agency Official for Privacy (SAOP) and Senior Procurement Executive or designee are designated to manage the development, documentation, and dissemination of the Department-level IT system and services acquisition policy.

This policy shall be reviewed and updated annually (i.e., each fiscal year) and following the identification of evolving threats, issuance of new or significantly changed existing Federal laws, executive orders, directives, regulations, and ED policies, identification of emerging technology and information technology service delivery models and determination that adjustments are deemed necessary to improve its effectiveness based upon feedback from Principal Office personnel.

Principal Office (PO) Information System Owners (ISO) and Information System Security Officers (ISSOs) are required to manage the development, documentation, and dissemination of system specific procedures to facilitate the implementation of this policy standard and associated system and services acquisition controls. The ISO and ISSO shall review system and services acquisition procedures annually (i.e., each fiscal year) and following the identification of evolving threats, issuance of new or significantly changed existing Federal laws, executive orders, directives, regulations, and ED policies, identification of emerging technology and information technology service delivery models and determination that adjustments are deemed necessary to improve its effectiveness based upon feedback from Principal Office personnel.

## **2.2 AU-02 Event Logging (P, L, M, H and Control Overlay)**

- a. Identify the types of events that the system is capable of logging in support of the audit function. The types of events shall include those events that are significant and relevant to the security of systems and the privacy of individuals and that provide the ability to establish, correlate, and investigate events relating to an incident or identify those responsible for one.

---

<sup>8</sup> Also known as OCIO: 3-110.

<sup>9</sup> Also known as OFO-F: 2-107.

- 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 event types for logging within the system, as required to comply with OMB Memorandum M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*, or successor.
- d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents.
- e. Review and update the event types selected for logging annually (i.e., each fiscal year) or whenever there is a change in Department policies and standards, system's threat environment, or tiers and maturity model for event log management published by OMB memo.

**Control Overlay AU-02 ED-01 (L, M, H):** Document the system logging maturity tier level quarterly in Cyber Security Assessment and Management (CSAM), upload or link one or more artifact in CSAM to provide evidence of stated level and associate the supporting artifact/evidence with this control. Maturity tier level is based on a 95% compliance<sup>10</sup> on a running two-week period.

**Control Overlay AU-02 ED-02 (L, M, H):** Configure logging to record the necessary information about security events involving EO-critical software platforms and all software running on those platforms.

### **2.3 AU-03 Content of Audit Records (L, M, H)**

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.

#### **2.3.1 AU-03(01) Content of Audit Records | Additional Audit Information (M,H)**

Generate audit records containing additional information as required to comply with OMB M-21-31 or successor.

---

<sup>10</sup> If a system drops below 95% asset reporting at any time during a two-week period their tier level is reduced to the next lower tier of compliance. For example, if an Event Logging Level 0 (EL0) system can maintain the requirements for Event Logging Level 1 (EL1) for two weeks at 95 percent of its required reporting elements functional, then that system would be considered EL1. Conversely, if an EL1 or Event Logging Level 2 (EL2) system suffers an outage or failure that causes the system to drop below 95 percent for required reporting elements for two weeks, then we would drop the system to EL0.



### **2.3.2 AU-03(03) Content of Audit Records | Limit Personally Identifiable Information Elements (P)**

Limit personally identifiable information contained in audit records to the elements identified in the privacy risk assessment authorized by the Department's SAOP.

### **2.4 AU-04 Audit Log Storage Capacity (L, M, H, and Control Overlay)**

Allocate audit log storage capacity to accommodate the reduction in the likelihood of such capacity being exceeded and resulting in the potential loss or reduction of audit logging capability. At a minimum, audit log storage capacity must comply with OMB M-21-31 or successor.

*Control Overlay AU-04 ED-01 (L, M, H):* Send logs to the Department's Cyber Data Lake (EDCDL) for storage.

### **2.5 AU-05 Response to Audit Logging Process Failures (L, M, H)**

- a. Alert Administrators (Application, System, Network, etc.) and ISSO, at a minimum, within a matter of minutes (i.e., real-time alerts) in the event of an audit logging process failure.
- b. Take the following additional actions, overwrite oldest audit records for those systems which are configured to offload audit logs to a separate system or shut down the information system when audit records are not offloaded to a separate system. Actions taken must comply with OMB M-21-31 or successor.

#### **2.5.1 AU-05(01) Response to Audit Logging Process Failures | Storage Capacity Warning (H)**

Provide a warning to Administrators (Application, System, Network, etc.) within an hour, when allocated audit log storage volume reaches 75% of repository maximum audit log storage capacity.

#### **2.5.2 AU-05(02) Response to Audit Logging Process Failures | Real-time Alerts (H)**

Provide an alert within an hour to Administrators (Application, System, Network, etc.) when the following audit failure events occur:

- a. Inability to forward audit logs to separate system
- b. Audit records overwritten
- c. Generation of audit logs stopped.

### **2.6 AU-06 Audit Record Review, Analysis, and Reporting (L, M, H and Control Overlay)**

- a. Review and analyze system audit records as required to comply with OMB M-21-31 or successor, for indications of compromise such as unauthorized access, unauthorized account additions or role modifications, misuse of authority or access, misconfiguration, unauthorized

modification or deletion of data and the potential impact of the inappropriate or unusual activity.

- b. Report findings to ISOs, ISSOs, and ED Security Operations Center (EDSOC) personnel.
- 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 Overlay AU-06 ED-01 (L, M, H):** Require the EDSOC to provide, upon request and to the extent consistent with applicable law, relevant logs to CISA and the Federal Bureau of Investigation.

**Control Overlay AU-06 ED-02 (L, M, H):** Share log information, as needed and appropriate with other Federal agencies to address cybersecurity risks or incidents; all log sharing with other Federal agencies must be conducted by or coordinated with the EDSOC.

### **2.6.1 AU-06(01) Audit Record Review, Analysis, and Reporting | Automated Process Integration (M, H)**

Integrate audit record review, analysis, and reporting processes using Department authorized automated tools with the ability to consolidate, analyze and report the results of audit record review as required to comply with OMB M-21-31 or successor.

### **2.6.2 AU-06(03) Audit Record Review, Analysis, and Reporting | Correlate Audit Record Repositories (M,H)**

The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.

### **2.6.3 AU-06(04) 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.

### **2.6.4 AU-06(05) Audit Record Review, Analysis, and Reporting | Integrated Analysis of Audit Records (H)**

Integrate analysis of audit records with analysis of vulnerability scanning information, performance data, system monitoring information, physical access control devices, and other systems within the system authorization boundary and/or hosting environment and other data and information as required to comply with OMB M-21-31 or successor, to further enhance the ability to identify inappropriate or unusual activity.

### **2.6.5 AU-06(06) Audit Record Review, Analysis, and Reporting | Correlation with Physical Monitoring (P)**

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.

### **2.6.6 AU-06(07) Audit Record Review, Analysis, and Reporting | Permitted Actions**

Specify the permitted actions for each role or user associated with the review, analysis, and reporting of audit record information.

### **2.6.7 AU-06(09) Audit Record Review, Analysis, and Reporting | Correlation with Information from Nontechnical Sources**

Correlate information from nontechnical sources with audit record information to enhance organization-wide situational awareness.

## **2.7 AU-07 Audit Recording Reduction and Report Generation (M, H)**

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.

### **2.7.1 AU-07(01) Audit Record Reduction and Report Generation | Automatic Processing (M, H)**

Provide and implement the capability to process, sort, and search audit records for events of interest based on the following content: system resources involved, information objects accessed, identities of individuals, event types, event locations, event dates and times, Internet Protocol (IP) addresses involved, or event success or failure and other content as required to comply with OMB M-21-31 or successor.

## **2.8 AU-08 Time Stamps (L, M, H)**

Use internal system clocks to generate time stamps for audit records. Record time stamps for audit records that meet requirements to comply with OMB M-21-31 or successor 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.

## **2.9 AU-09 Protection of Audit Information (L, M, H)**

Protect audit information and audit logging tools from unauthorized access, modification, and deletion. Alert the ISO, ISSO, and EDSOC upon detection of unauthorized access, modification, or deletion of audit information.

**2.9.1 AU-09(02) Protection of Audit Information | Store on Separate Physical Systems or Components (H)**

Store audit records as required to comply with OMB M-21-31 or successor, in a repository that is part of a physically different system or system component than the system or component being audited.

**2.9.2 AU-09(03) Protection of Audit Information | Cryptographic Protection (H and Control Overlay)**

Implement cryptographic mechanisms to protect the integrity of audit information and audit tools.

*Control Overlay AU-09(03) ED-01 (L, M, H):* Employ cryptographic mechanisms to protect the integrity of audit information related to HVA.

**2.9.3 AU-09(04) Protection of Audit Information | Access by Subset of Privileged Users (M, H)**

Authorize access to management of audit logging functionality to only a subset of privileged users, as required to comply with OMB M-21-31 or successor.

**2.9.4 AU-09(05) Protection of Audit Information | Dual Authorization**

Enforce dual authorization for manual movement and deletion of system audit logs.

**2.9.5 AU-09(06) Protection of Audit Information | Read-Only Access**

Authorize read-only access to audit information to system-identified and documented privileged accounts only.

**2.10 AU-10 Non-repudiation (H)**

Provide irrefutable evidence that an individual (or process acting on behalf of an individual) has performed actions sufficient to prove user non-repudiation as required to comply with OMB M-21-31 or successor.

**2.11 AU-11 Audit Record Retention (P, L, M, H)**

Retain audit records for time frames required to comply with OMB M-21-31 or successor, to provide support for after-the-fact investigations of incidents and to meet statutory, regulatory, and organizational information retention requirements.

**2.12 AU-12 Audit Record Generation (L, M, H)**

- a. Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2a on all system components.
- b. Allow ISOs and ISSOs in accordance with OMB M-21-31 or successor to select the event types that are to be logged by specific components of the system.

- c. Generate audit records for the event types defined in AU-2c that include the audit record content defined in AU-3.

#### **2.12.1 AU-12(01) Audit Record Generation | System-wide and Time-correlated Audit Trail (H)**

Compile audit records from all system components into a system-wide (logical or physical) audit trail that is time-correlated to within a timeframe as required to comply with OMB M-21-31 or successor.

#### **2.12.2 AU-12(03) Audit Record Generation | Changes by Authorized Individuals (H)**

Provide and implement the capability for Administrators (Application, System, Network, etc.), ISO, ISSO, Information System Security Manager (ISSM), System Program/Project Managers to change the logging to be performed on all system components based on change management decisions or threat criteria provided by the EDSOC and as required to comply with OMB M-21-31 or successor within one hour.

### **2.13 AU-16 Cross-Organizational Audit Logging**

Employ contracts or agreements for coordinating audit information among external organizations when audit information is transmitted across organizational boundaries.

#### **2.13.1 AU-16(01) Cross-Organizational Audit Logging | Identity Preservation**

Preserve the identity of individuals in cross-organizational audit trails.

#### **2.13.2 AU-16(02) Cross-Organizational Audit Logging | Sharing of Audit Information**

Provide cross-organizational audit information to authorized organizations based on cross-organizational sharing agreements.

### **3 RISK ACCEPTANCE/POLICY EXCEPTIONS**

Deviations from the Department policies, Instructions, Standards, Procedures or Memos must be approved and documented through the Department's Risk Acceptance process. Deviations that introduce additional risks to the enterprise must be submitted through the Department Risk Acceptance Form (RAF) and must be approved by the ED CISO (as delegated). Requests must justify the reason for the deviation(s)/exception(s) as well as the compensating security controls implemented to secure the device or information, if applicable. Policy deviations that do not introduce additional risks do not need to be submitted through the Department RAF but will need to be approved by the Department CISO (as delegated).

## 4 ACRONYMS

Acronym	Definition
ACSD	Administrative Communications System Directives
AU	System Audit and Accountability Family
BOD	Binding Operational Directive
CIO	Chief Information Officer
CISA	Cybersecurity & Infrastructure Security Agency
CISO	Chief Information Security Officer
CSAM	Cyber Security Assessment and Management
CSF	Cybersecurity Framework
Department	U.S. Department of Education
DHS	U.S. Department of Homeland Security
ED	U.S. Department of Education
EDCDL	ED Cyber Data Lake
EDSOC	ED Security Operations Center
EL0	Event Logging Level 0
EL1	Event Logging Level 1
EL2	Event Logging Level 2
EO	Executive Order
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Modernization Act
FTRI	Federal Tax Return Information
GRP	Governance, Risk and Policy
H	High
HVA	High Value Asset
IAS	Information Assurance Services
IP	Internet Protocol
IRS	Internal Revenue Service
ISO	Information System Owner
ISSM	Information System Security Manager
ISSO	Information System Security Officer
IT	Information Technology
L	Low
M	Moderate
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
ODP	Organizationally Defined Parameters
OMB	Office of Management and Budget
P	Privacy
PF	Privacy Framework
PO	Principal Office
PUB	Publication
RAF	Risk Acceptance Form
SAOP	Senior Agency Official for Privacy

Acronym	Definition
SP	Special Publication
CT-P	Control-P
DE	Detect
GV-P	Govern-P
ID	Identify
ID-P	Identify-P
PR	Protect
PR-P	Protect-P
RS	Respond
CT.DM-P	Data Processing Management
CT.DP-P	Disassociated Processing
DE.AE	Anomalies and Events
DE.CM	Security Continuous Monitoring
DE.DP	Detection Processes
GV.MT-P	Monitoring and Review
GV.PO-P	Governance Policies, Processes, and Procedures
ID.DE-P	Data Processing Ecosystem Risk Management
ID.SC	Supply Chain Risk Management
PR.DS	Data Security
PR.DS-P	Data Security
PR.PT	Protective Technology
RS.AN	Analysis
RS.CO	Communications



## APPENDIX A - BASELINE CONTROL PARAMETER SUMMARY

The applicability for each baseline control parameter is shown below.

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and PF Category	CSF and PF Subcategory
AU-1	Policy and Procedures	X	X	X	X	PR.PT, DE.DP, GV.PO-P, GV.MT-P, CT.DM-P	PR.PT-1, DE.DP-2, GV.PO-P1, GV.PO-P3, GV.PO-P5, GV.MT-P2, GV.MT-P6, CT.DM-P8
AU-2	Event Logging	X	X	X	X	PR.PT, CT.DM-P	PR.PT-1, CT.DM-P8
AU-3	Content of Audit Records		X	X	X	PR.PT, CT.DM-P, CT.DP-P	PR.PT-1, CT.DM-P8, CT.DP-P2
AU-3(1)	Content of Audit Records   Additional Audit Information			X	X	PR.PT, CT.DM-P, CT.DP-P	PR.PT-1, CT.DM-P8, CT.DP-P2
AU-3(3)	Content of Audit Records   Limit Personally Identifiable Information Elements	X				PR.PT, CT.DM-P, CT.DP-P	PR.PT-1, CT.DM-P8, CT.DP-P2
AU-4	Audit Log Storage Capacity		X	X	X	PR.DS, PR.DS-P	PR.DS-4, PR.DS-P4
AU-4(1)	Audit Log Storage Capacity   Transfer to Alternate Storage					PR.DS, PR.DS-P	PR.DS-4, PR.DS-P4
AU-5	Response to Audit Logging Process Failures		X	X	X		
AU-5(1)	Response to Audit Logging Process Failures   Storage Capacity Warning				X		
AU-5(2)	Response to Audit Logging Process Failures   Real-time Alerts				X		
AU-5(3)	Response to Audit Logging Process Failures   Configurable Traffic Volume Thresholds						
AU-5(4)	Response to Audit Logging Process Failures   Shutdown on Failure						
AU-5(5)	Response to Audit Logging Process Failures   Alternate Audit Logging Capability						
AU-6	Audit Record Review, Analysis, and Reporting		X	X	X	ID.SC, PR.PT, DE.AE,	ID.SC-4, PR.PT-1, DE.AE-2,

Information Technology (IT) Audit and Accountability (AU) Standard

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and PF Category	CSF and PF Subcategory
						DE.DP, RS.CO, RS.AN, ID.DE-P, CT.DM-P	DE.AE-3, DE.DP-4, RS.CO-2, RS.AN-1, ID.DE-P5, CT.DM-P8
AU-6(1)	Audit Record Review, Analysis, and Reporting   Automated Process Integration			X	X	ID.SC, PR.PT, DE.AE, DE.DP, RS.CO, RS.AN, ID.DE-P, CT.DM-P	ID.SC-4, PR.PT-1, DE.AE-2, DE.AE-3, DE.DP-4, RS.CO-2, RS.AN-1, ID.DE-P5, CT.DM-P8
AU-6(3)	Audit Record Review, Analysis, and Reporting   Correlate Audit Record Repositories			X	X	ID.SC, PR.PT, DE.AE, DE.DP, RS.CO, RS.AN, ID.DE-P, CT.DM-P	ID.SC-4, PR.PT-1, DE.AE-2, DE.AE-3, DE.DP-4, RS.CO-2, RS.AN-1, ID.DE-P5, CT.DM-P8
AU-6(4)	Audit Record Review, Analysis, and Reporting   Central Review and Analysis					ID.SC, PR.PT, DE.AE, DE.DP, RS.CO, RS.AN, ID.DE-P, CT.DM-P	ID.SC-4, PR.PT-1, DE.AE-2, DE.AE-3, DE.DP-4, RS.CO-2, RS.AN-1, ID.DE-P5, CT.DM-P8
AU-6(5)	Audit Record Review, Analysis, and Reporting   Integrated Analysis of Audit Records				X	ID.SC, PR.PT, DE.AE, DE.DP, RS.CO, RS.AN, ID.DE-P, CT.DM-P	ID.SC-4, PR.PT-1, DE.AE-2, DE.AE-3, DE.DP-4, RS.CO-2, RS.AN-1, ID.DE-P5, CT.DM-P8
AU-6(6)	Audit Record Review, Analysis, and Reporting   Correlation with Physical Monitoring				X	ID.SC, PR.PT, DE.AE, DE.DP, RS.CO, RS.AN, ID.DE-P, CT.DM-P	ID.SC-4, PR.PT-1, DE.AE-2, DE.AE-3, DE.DP-4, RS.CO-2, RS.AN-1, ID.DE-P5, CT.DM-P8

Information Technology (IT) Audit and Accountability (AU) Standard

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and PF Category	CSF and PF Subcategory
AU-6(7)	Audit Record Review, Analysis, and Reporting   Permitted Actions					ID.SC, PR.PT, DE.AE, DE.DP, RS.CO, RS.AN, ID.DE-P, CT.DM-P	ID.SC-4, PR.PT-1, DE.AE-2, DE.AE-3, DE.DP-4, RS.CO-2, RS.AN-1, ID.DE-P5, CT.DM-P8
AU-6(8)	Audit Record Review, Analysis, and Reporting   Full Text Analysis of Privileged Commands					ID.SC, PR.PT, DE.AE, DE.DP, RS.CO, RS.AN, ID.DE-P, CT.DM-P	ID.SC-4, PR.PT-1, DE.AE-2, DE.AE-3, DE.DP-4, RS.CO-2, RS.AN-1, ID.DE-P5, CT.DM-P8
AU-6(9)	Audit Record Review, Analysis, and Reporting   Correlation with Information from Nontechnical Sources					ID.SC, PR.PT, DE.AE, DE.DP, RS.CO, RS.AN, ID.DE-P, CT.DM-P	ID.SC-4, PR.PT-1, DE.AE-2, DE.AE-3, DE.DP-4, RS.CO-2, RS.AN-1, ID.DE-P5, CT.DM-P8
AU-7	Audit Record Reduction and Report Generation			X	X	PR.PT, RS.AN, CT.DM-P	PR.PT-1, RS.AN-3, CT.DM-P8
AU-7(1)	Audit Record Reduction and Report Generation   Automatic Processing			X	X	PR.PT, RS.AN, CT.DM-P	PR.PT-1, RS.AN-3, CT.DM-P8
AU-8	Time Stamps		X	X	X		
AU-9	Protection of Audit Information		X	X	X		
AU-9(1)	Protection of Audit Information   Hardware Write-once Media						
AU-9(2)	Protection of Audit Information   Store on Separate Physical Systems or Components				X		
AU-9(3)	Protection of Audit Information   Cryptographic Protection				X		
AU-9(4)	Protection of Audit Information   Access by Subset of Privileged Users			X	X		

Information Technology (IT) Audit and Accountability (AU) Standard

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and PF Category	CSF and PF Subcategory
AU-9(5)	Protection of Audit Information   Dual Authorization						
AU-9(6)	Protection of Audit Information   Read-only Access						
AU-9(7)	Protection of Audit Information   Store on Component with Different Operating System						
AU-10	Non-repudiation				X		
AU-10(1)	Non-repudiation   Association of Identities						
AU-10(2)	Non-repudiation   Validate Binding of Information Producer Identity						
AU-10(3)	Non-repudiation   Chain of Custody						
AU-10(4)	Non-repudiation   Validate Binding of Information Reviewer Identity						
AU-11	Audit Record Retention	X	X	X	X		
AU-11(1)	Audit Record Retention   Long-term Retrieval Capability						
AU-12	Audit Record Generation		X	X	X	PR.PT, DE.CM, CT.DM-P	PR.PT-1, DE.CM-1, DE.CM-3, DE.CM-7, CT.DM-P6, CT.DM-P8
AU-12(1)	Audit Record Generation   System-wide and Time-correlated Audit Trail				X	PR.PT, DE.CM, CT.DM-P	PR.PT-1, DE.CM-1, DE.CM-3, DE.CM-7, CT.DM-P6, CT.DM-P8
AU-12(2)	Audit Record Generation   Standardized Formats					PR.PT, DE.CM, CT.DM-P	PR.PT-1, DE.CM-1, DE.CM-3, DE.CM-7, CT.DM-P6, CT.DM-P8
AU-12(3)	Audit Record Generation   Changes by Authorized Individuals				X	PR.PT, DE.CM, CT.DM-P	PR.PT-1, DE.CM-1, DE.CM-3, DE.CM-7, CT.DM-P6, CT.DM-P8

Information Technology (IT) Audit and Accountability (AU) Standard

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and PF Category	CSF and PF Subcategory
AU-12(4)	Audit Record Generation   Query Parameter Audits of Personally Identifiable Information					PR.PT, DE.CM, CT.DM-P	PR.PT-1, DE.CM-1, DE.CM-3, DE.CM-7, CT.DM-P6, CT.DM-P8
AU-13	Monitoring for Information Disclosure					PR.DS, PR.PT, DE.CM, CT.DM-P, PR.DS-P	PR.DS-5, PR.PT-1, DE.CM-3, CT.DM-P8, PR.DS-P5
AU-13(1)	Monitoring for Information Disclosure   Use of Automated Tools					PR.DS, PR.PT, DE.CM, CT.DM-P, PR.DS-P	PR.DS-5, PR.PT-1, DE.CM-3, CT.DM-P8, PR.DS-P5
AU-13(2)	Monitoring for Information Disclosure   Review of Monitored Sites					PR.DS, PR.PT, DE.CM, CT.DM-P, PR.DS-P	PR.DS-5, PR.PT-1, DE.CM-3, CT.DM-P8, PR.DS-P5
AU-13(3)	Monitoring for Information Disclosure   Unauthorized Replication of Information					PR.DS, PR.PT, DE.CM, CT.DM-P, PR.DS-P	PR.DS-5, PR.PT-1, DE.CM-3, CT.DM-P8, PR.DS-P5
AU-14	Session Audit					PR.PT, CT.DM-P	PR.PT-1, CT.DM-P8
AU-14(1)	Session Audit   System Start-up					PR.PT, CT.DM-P	PR.PT-1, CT.DM-P8
AU-14(3)	Session Audit   Remote Viewing and Listening					PR.PT, CT.DM-P	PR.PT-1, CT.DM-P8
AU-16	Cross-organizational Audit Logging					PR.PT, CT.DM-P, CT.DP-P	PR.PT-1, CT.DM-P8, CT.DP-P1, CT.DP-P3
AU-16(1)	Cross-organizational Audit Logging   Identity Preservation					PR.PT, CT.DM-P, CT.DP-P	PR.PT-1, CT.DM-P8, CT.DP-P1, CT.DP-P3
AU-16(2)	Cross-organizational Audit Logging   Sharing of Audit Information					PR.PT, CT.DM-P, CT.DP-P	PR.PT-1, CT.DM-P8, CT.DP-P1, CT.DP-P3
AU-16(3)	Cross-organizational Audit Logging   Disassociability					PR.PT, CT.DM-P, CT.DP-P	PR.PT-1, CT.DM-P8, CT.DP-P1, CT.DP-P3