Division of Enterprise Technology Strategy and Services

ETSS Policy 300.3

Audit and Accountability (AU)

Publish Date: 23 June 2026
Effective Date: 23 June 2026
Last Review: 22 June 2026

doa.entsec@doit.ri.gov

1. Purpose

Establish policy for effectively managing and monitoring audit and accountability controls to ensure there are sufficient information system logs of actions performed to determine accountability.

2. Applicability

This policy is applicable to all State of Rhode Island Executive Branch Departments[1] (including agencies, boards and commissions), and their employees (including permanent, non-permanent, full-time, and part-time) and interns, consultants, contractors, vendors, contracted individuals, and any entity having access to state information systems and data, whether operated or maintained by the state or on behalf of the state. For this policy, the term "agency" is used to refer to any department, agency, division, or unit of the Executive branch of the State of Rhode Island.

3. Definitions

Auditable Event
An observable occurrence identified for its significance and relevance to the security of the information system and environment in which it operates (e.g. user logins/logoffs, system administrator activities).

Audit Reduction
A process that manipulates and organizes audit record data to provide analysts with more useful and meaningful information within audit reports during reviews.

Non-Repudiation
Ensuring that a user or process cannot falsely deny having performed an action.

Moderate Risk Systems (IAL2)
Information systems that store, process, transfer, or communicate private or sensitive data or have a direct dependency on a Moderate system. At a minimum, any information system that stores, processes, transfers, or communicates PII or other sensitive data types is classified as a Moderate system.

***3.1. [IAL1, IAL2]* Audit and Accountability Policy and Procedures (AU-1).** The agency will develop, document, disseminate to designated personnel defined in the applicable system security plan (SSP), review, and annually update an audit and accountability policy and procedures.

***3.2. [IAL1, IAL2]* Event Logging (AU-2).** The agency will:

1. Identify the types of events that the information system can log. Where possible, *Center for Internet Security (CIS) Benchmarks* level 1 audit event logging recommendations should be implemented. At a minimum, the information system will log ALL:
- ***a.*** Successful and failed authentication attempts.
- ***b.*** Logons and logoffs.
- ***c.*** Activities of privileged users (e.g. system and network administrators).
- ***d.*** Changes to user accounts, access permissions, passwords, and system/application configurations (e.g. create, modify, delete).
- ***e.*** Changes to security functions (e.g. disabling logging, password criteria).
- ***f.*** Changes to network configurations (e.g. routers, firewalls, switches, proxies, servers).
- ***g.*** Batch file changes to applications and databases.
- ***h.*** System and application startups, shutdowns, restarts, reboots, alerts, and errors.
- ***i.*** Switching accounts or running privileged actions from another account (e.g. Linux/UNIX SU or Windows RUNAS).
- ***j.*** Remote access to the state network.
- ***k.*** In addition to the above events, for network perimeter devices (e.g. firewalls, routers):
  - ***i.*** Log packet-screening denials originating from untrusted networks.
  - ***ii.*** Blocked or denied network traffic from internal or trusted networks, including policy violations, misconfigurations, or potentially malicious activity originating from inside the environment.
  - ***iii.*** Creation, modification, or removal of network security rules, including firewall rules, security group rules, access control lists (ACLs), or other traffic-filtering configurations.
  - ***iv.*** Changes to proxy, secure web gateway, or traffic inspection services, including configuration changes that affect how network traffic is filtered, inspected, or routed.
- ***l.*** Any event determined by the agency after reviewing its business processes, compliance requirements, and information system capabilities to be relevant to the security of the information system and required by its regulatory environment.

2. Audit events within the logging frequency or situational awareness, as determined by the agency, that is required for each identified event type. For events identified in a-k of section 1 above, every occurrence of these events will be logged.

3. Coordinate the event logging function with other agencies, as appropriate.

4. Provide rationale for why events selected for logging are deemed adequate to support after-the-fact investigations of incidents. For the events identified above, the rationale behind selecting the events is to ensure the confidentiality, integrity, and availability of the information system,

network, and data and ensure that mission critical information systems and data are not corrupted and remain available. By logging and auditing these events, the security of information systems, network, and data is increased. At a minimum, audit event will be reviewed to identify:

a. Possible credential theft or compromised identifiers or authenticators.
b. Unauthorized access or access that is performed during non-business or non-regularly scheduled hours.
c. Possible insider threats.
d. Unauthorized privileged user actions, either inadvertent or malicious.
e. Unauthorized accounts, permissions, or configurations.
f. Unauthorized network and infrastructure changes, which increase the risk of a system or data compromise.
g. Unauthorized changes to automated script and batch files.
h. Problems within information systems and network components prior to critical failures.

5. Review and update the list of selected events annually or whenever there is a change in the threat environment. The system owner is responsible for reviewing and updating the list of auditable events that are not inherited from the enterprise.

3.3. [IAL1, IAL2] **Content of Audit Records (AU-3).** The information system will generate audit records that establish the following:

1. Type of event that occurred (e.g. type/description).
2. When the event occurred (e.g. date/time).
3. Where the event occurred (e.g. source/destination IP).
4. Source of the event (e.g. user/process).
5. Outcome of the event (e.g. success/failure).
6. Identity of any individuals, subjects, objects, or entities associated with the event.

> ***[IAL2]*** **Additional Audit Information (AU-3.1).** The information system will generate records containing additional audit information that agency business, system, or data owners have identified as necessary (e.g. reconstruct chronological order of activities leading to an event/fraud, provide non-repudiation of all actions performed, provide full context of transactions entered into the system). Additional audit information being logged will be documented in the SSP. Examples of additional audit information includes, but is not limited to, name of file being accessed, program or command used to initiate an event, duration of the session/connection/transaction/activity, bytes sent/received, diagnostic messages, or characteristics (e.g. type/location/subject) of the resource being acted upon.

3.4. [IAL1, IAL2] **Audit Log Storage Capacity (AU-4).** The agency will allocate adequate audit record storage capacity necessary to maintain the logs of all auditable records in accordance with ETSS minimum standards defined in ETSS Asset Log Retention and Management Standard and superseded where precedent is set by State or Federal regulation. For more information that may assist in determining the appropriate size of audit record storage capacity, see *State of RI Department of State General Record Schedule GRS7*.

3.5. [IAL1, IAL2] **Response to Audit Logging Process Failures (AU-5).** The agency will:

1. Develop procedures for handling audit processing failures that are appropriate for the information system and its business process. At a minimum, the system administrator will monitor the operational status, functions, and performance of the information system via system audit logs that identify system process failures and provide information relative to corrective actions to be taken by the system administrator.
2. Alert designated personnel, defined in the applicable SSP, in the event of an audit logging process failure. Alerts will be distributed via a method that ensures designated personnel receive the alerts both on and off hours (e.g. phone call, text message, email). At a minimum, alerts will be sent to designated personnel when the following audit processing failures occur:
   a. Auditable events are not being logged.
   b. Audit log records are being overwritten.
   c. Audit log record storage capacity utilization reaches 75%, 90%, and 100%. The information system will overwrite the oldest audit records or shut down, as appropriate, when maximum audit record storage capacity is reached.

3.6. ***[IAL1, IAL2]*** **Audit Record Review, Analysis, and Reporting (AU-6).** The agency should review applicable federal and state laws, regulations, mandates, and compliance requirements to determine appropriate audit record review timeframes. The agency will:

1. Review and analyze audit records for potential impact and indications of inappropriate, unusual, or suspicious activity, including:
   a. Real-time (or as close to real-time as possible) review of system and application errors and alerts. Errors and alerts for IAL2 moderate risk information systems take precedence over IAL1 low risk information systems.
   b. Daily review of initialization sequences, logons, and errors.
   c. Daily review of system processes and performance.
   d. Daily review of system resource utilization.
   e. Daily review of network traffic, bandwidth utilization rates, alert notifications, and border defense devices.
   f. For external service providers, weekly review of audit records relevant to maintain confidentiality, integrity, and availability of agency data hosted on external service provider systems. Reviewable audit records should be defined within the SLA. An external service provider attestation that relevant audit records have been reviewed, including the results of the review, satisfies this requirement.
   g. Monthly review of administrator groups (e.g. to identify unauthorized administrator accounts).
2. Forward audit records of information systems deemed high-risk and/or mission-critical the Enterprise Security Information and Event Management (SIEM). If unable to do so, the agency will document this risk within the information system SSP.
3. Report findings to designated personnel, defined in the applicable SSP. Actual or suspected security incidents will be handled in accordance with *ETSS Incident Handling and Response Policy 10-12* and escalated to the ETSS SOC immediately for review. .
4. Adjust the level of audit reviews, analysis, and reporting when there is a change within the threat environment based on law enforcement, intelligence information, and other credible sources of information.

3.6.1. [IAL2] **Automated Process Integration (AU-6.1).** The agency will employ automated mechanisms to integrate the audit review, analysis, and reporting processes into incident response, continuous monitoring, and contingency planning activities to support agency processes for investigation and response to suspicious activities.

3.6.2. [IAL2] **Correlate Audit Record Repositories (AU-6.3).** The agency will analyze and correlate audit records across different log repositories to investigate and respond to indications of unlawful, unauthorized, suspicious, or unusual activity and gain insight into agency and enterprise-wide risk management and situational awareness. The Enterprise SIEM solution may aid in correlating and analyzing audit repositories.

3.7. [IAL2] **Audit Record Reduction and Report Generation (AU-7).** Audit reduction is a process that manipulates collected audit information and organizes this information within a summary format that is more meaningful to analysts. Audit reduction capabilities include modern data mining techniques with advanced filters that identify anomalous behavior within audit records. The agency will provide an audit reduction and report generation capability that:

1. Supports on-demand audit review, analysis, reporting, and after-the-fact investigations of security incidents.

2. Does not alter the contents or time ordering of audit records.

3.7.1. [IAL2] **Automatic Processing (AU-7.1).** The agency will provide the capability to automatically process, sort, and search audit records for events of interest based on audit fields within audit records, including as system resources involved, objects accessed, identities of individuals, IP addresses, or event types/locations/ dates/ times/successes/failures. Automated correlation and advanced analytics will be implemented where supported by enterprise tooling or approved system-specific solutions. Limitations must be documented in the SSP.

3.8. [IAL1, IAL2] **Time Stamps (AU-8).** The agency will:

1. Use internal system clocks to generate audit record time stamps.

2. Record time stamps for audit records that meet appropriate time stamp granularity requirements for the information system 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 expressed in local time with an offset from Coordinated Universal Time (UTC). Unless the system is unable to do so, the information system will synchronize internal system clocks to a centralized Enterprise Network Time Protocol (NTP) time server.

3.9. [IAL1, IAL2] **Protection of Audit Information (AU-9).** The agency will:

1. Protect audit information (e.g. audit records, settings, reports) and audit logging tools from unauthorized access, modification, and deletion. Cryptographic mechanisms are implemented to protect the confidentiality and integrity of audit information and audit tools. Audit records will be read-only and not modified or deleted at any time prior to the end of the retention period. Audit records will be backed up on a system other than the one being audited.

2. Alert designated personnel (e.g. system administrators, security personnel) upon detection of unauthorized access, modification, or deletion of audit information.

***3.9.1. [IAL2]* Access by Subset of Privileged Users (AU-9.4).** The agency will authorize access to manage audit functionality only to designated privileged users and security administrators. System and network administrators will not have the ability to modify or delete audit records except where platform constraints require administrative access, in which case compensating controls must be documented in the SSP and approved by the CISO. Separation of duties will be enforced such that personnel who administer the access control function are different than those who administer or have access to audit record data. Audit record repositories and backup log archives will be accessible only to authorized personnel and be protected from breaches of confidentiality or integrity.

***3.10. [IAL1, IAL2]* Audit Record Retention (AU-11).** The agency will retain audit records in accordance with all applicable federal and state laws, regulations, mandates, and compliance requirements to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements. For more information regarding audit record retention requirements, see *State of Rhode Island Department of State General Record Schedule GRS7*. FTI-related audit trail records will be retained for seven (7) years. In the absence of any documented retention requirements, audit records will be retained for a minimum of six (6) months.

***3.11. [IAL1, IAL2]* Audit Record Generation (AU-12).** The agency will:

1. Provide audit record generation capability for the auditable events defined in control AU-2 of this policy for all information systems and system components including, but not limited to, desktops and laptops (end-users), network devices (e.g. routers, switches, firewalls, intrusion detection), servers (e.g. file, print, web, terminal), mainframes, and databases.
2. Allow designated personnel (e.g. system administrators, security personnel) to select the types of events that are to be logged by specific components of the system.
3. Generate audit records for events defined in control AU-2 of this policy that include the content defined in control AU-3 of this policy.

4. Approval / Review Signature:

Sanjay Gupta
Digitally signed by Sanjay Gupta
Date: 2026.06.22 16:37:32 -04'00'

Chief Technology Officer (CTO)
Division of Enterprise Technology Strategy and Services (ETSS)

Digitally signed by Nathan Loura
Date: 2026.06.23 12:24:53 -04'00'

Chief Information Security Officer (CISO)
Division of Enterprise Technology Strategy and Services (ETSS)

Brian Tardiff
Digitally signed by Brian Tardiff
Date: 2026.06.23 12:43:04 -04'00'

Chief Digital Officer (CDO)
Division of Enterprise Technology Strategy and Services (ETSS)