



STATE OF ALABAMA

OFFICE OF INFORMATION TECHNOLOGY



STANDARD 645S1: Audit Requirements

VERSION NUMBER	Standard 645S1-01
VERSION DATE	July 9, 2020
STANDARD TITLE	Audit Requirements
GOVERNING POLICY	This standard is governed by Policy 645: Audit and Accountability, regardless of revision.
OBJECTIVE	Information system owners will make their own decisions regarding the threats they face, their risk tolerance, and which audit policy settings they choose. The objective of this standard is to establish the minimum baseline requirements for collecting, storing, analyzing and disposing of audit logs generated by information systems operating on the enterprise network.
REQUIREMENTS	<ol style="list-style-type: none">1. AUDIT MANAGEMENT INFRASTRUCTURE<ol style="list-style-type: none">1.1. The log management infrastructure generally consists of the hardware, software, networks, and media used to generate, transmit, store, analyze, and dispose of log data.1.2. Log management architecture is generally composed of three tiers:<ol style="list-style-type: none">1.2.1. The first-tier, log generation, contains host (computers, network equipment, etc.) that generate log data utilized for conducting network and security audits.1.2.2. The second-tier, log analysis and storage, are comprised of one or more log servers that receive log data or copies of log data from a host (log generator) in the first tier. The data is transferred in either real-time or near real-time, or in occasional batches based on a schedule or the amount of log data waiting to be transferred. Servers that receive log data from multiple generators are designated as collectors or aggregators.1.2.3. The third-tier, log monitoring, contains consoles that may be used to monitor and review log data and the results or automated analysis.

1.3. Security Information and Event Management (SIEM) Software:

- 1.3.1. SIEM software has the capability to monitor and perform log analysis of information system events in real time or near real time. OIT Security Operations Center (SOC) personnel utilize a SIEM system when conducting audits of log data from various systems and network components.
- 1.3.2. The SIEM shall be configured to receive data from critical infrastructure via an installed agent (agent-based) or SYSLOG on the host. Non-critical systems may be agentless to reduce resource strain on information systems and volume of log data transferred over the network. [AU-12]
- 1.3.3. The SIEM shall be configured to alert security administrators when log data has ceased unexpectedly from critical infrastructure with installed agents. [AU-5a.]

2. AUDIT GENERATION

- 2.1. Not all information system events merit continuous logging activity or transfer in real-time or near real-time. Excessive logging should be avoided as it can cause operational problems such as system slowdowns or denial of service. Agency information system owners, data owners, and system administrators in collaboration with SOC personnel shall conduct risk assessments to determine the host, host components (OS, anti-virus, applications, services), and events that need to be logged for audit purposes. [CA-7] [RA-3]
- 2.2. System administrators shall consider the effect of the log source configuration on the logging host and other log management infrastructure components. Configure log sources to capture events from identified hosts in addition to determining the types of events each log source must log and data characteristics that must be logged for each type of event. For example:
 - 2.2.1. Domain controllers, servers, network components (switches, routers, firewalls) and other identified critical system from risk assessments shall have log data transferred in real-time or near real-time for analysis by SIEM automated applications.
 - 2.2.2. Non-critical systems (i.e., workstations) log data is not necessary to be transferred in real-time or near real-time

unless deemed otherwise by system administrators. The log data can be pulled (Agentless) from the system by the SIEM server to perform filtering, aggregation, log normalization, and analysis on the collected logs.

2.3. Determine that the information system is capable, at a minimum, of auditing the following event types: [AU-2a.]

- Startup and shutdown of audit functions
- Successful and unsuccessful logon/logoff
- Excessive logon attempts
- Log information on read, modify, delete operations
- Attempts to access security related files, utilities, and user authentication information
- Configuration changes executed during audit operations
- Changes/updates to internal system clock time
- Modification of system security controls
- Successful and unsuccessful privileged user account logon/logoff
- Addition/deletion to administrator groups
- Role modification of user groups
- Failure of log storage or exceeding log file threshold
- Software or application installations
- Blocking or blacklisting of user, system accounts or access port
- Modification of system files

Agencies may define additional events to be audited.

2.4. Minimum required logging events by host are [AU-2d.]:

Host	Event Category	Event
Domain Controllers	Policy change Account logon	Success/ Failure
Domain Controllers/ Member Servers	System	Success/ Failure
Domain Controllers/ Member Servers	Account Management	Success
SYSLOG Devices	Codes 0 through 6 Code 7-DEBUG optional	All
Mainframe and RACF	All	Selected Success/ Failure

- 2.5. The following hosts and audit events shall be logged, and these logs shall be forwarded to the OIT SOC:
- 2.5.1. Security Devices: All logs
 - 2.5.2. Windows Endpoints / Servers: Security logs
 - 2.5.3. Unix / Linux: Security and Authentication logs
 - 2.5.4. Routing / Switching: Security and Authentication logs
 - 2.5.5. Email: Security and Message Trace logs
 - 2.5.6. Applications: Security logs and logs deemed necessary based on assessment [AU-2d.]
- 2.6. Log data shall be generated for collection in its original format and forwarded to the SIEM for normalization, reduction, and report building for analysis. [AU-7]
- 2.7. Logs shall contain sufficient information for audit actions to be effective. Agency system administrators shall configure systems to log the following at a minimum:
- Type of event occurred
 - Date/time of event (check time of audit record host to ensure it is synchronized with established time controller system)
 - Where the event occurred
 - Source of event
 - Outcome of the event (success or failure) [AU-3]

3. AUDIT RECORD TIME STAMPS

- 3.1. Information systems shall use internal clocks to generate time stamps for audit records. [AU-8a.]
- 3.2. Time stamps for audit records shall be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT). [AU-8b.]
- 3.3. For systems and audit records that will be forwarded to the OIT, the internal information system clock shall be synchronized with the OIT enterprise time source or an OIT Domain Controller.

4. AUDIT SYSTEM CONFIGURATION

- 4.1. SIEM systems and audit tools shall be hardened, resistant to cyber-attack, with restricted physical and remote access, yet provide rapid access to current information for security analysis and management support. [PL-8 (CE1)]

- 4.2. Network communication between agents and the SIEM servers shall occur over a reliable TCP session and be encrypted. [SC-8]
- 4.3. System administrators may be required to configure agents on hosts prior to communicating with authenticated SIEM or audit servers before data transfer can be successful. [CM-6a., CM-6b.]

5. AUDIT RECORD STORAGE AND DISPOSAL

5.1. Retention:

- 5.1.1. To support audit or cyber incident event analysis, retain logs for at least one year or longer when required to meet regulatory audit record retention requirements. [AU-11]
- 5.1.2. Audit records involving Federal Tax Information (FTI) shall be maintained for seven (7) years or in accordance with the agency records disposition schedule, whichever is longer. [AU-11]
- 5.1.3. Logs pertaining to cybersecurity incidents shall be preserved in accordance with agency incident handling procedures. [IR-4a.]

5.2. Storage Capacity:

- 5.2.1. To reduce the probability of exceeding auditing capacity and to mitigate potential loss of auditing capability, allocate sufficient audit log storage capacity and configure logging to prevent storage capacity from being exceeded. [AU-4]
- 5.2.2. Information systems shall be configured to alert system, network, or security administrators to take appropriate action during audit failure or log storage capacity being reached to prevent logging capability shutdown. [AU-5]

5.3. Protection:

- 5.3.1. Audit information and audit tools shall be considered sensitive and afforded protection accordingly. Protect audit information and audit tools from unauthorized access, modification, or deletion. [AU-9]
- 5.3.2. Unauthorized access or attempted unauthorized access to log data may indicate a cyber-attack and shall be treated as a cybersecurity incident. [AU-9]

5.3.3. If log files contain personally identifiable information (PII), the agency shall ensure the privacy of log information is protected in accordance with applicable state standards for sensitive data or PII. Personnel responsible for privacy rule compliance for an agency should be consulted as part of log management planning. [AU-9]

5.3.4. This requirement applies to outsourced data centers or cloud providers: When audit information is transmitted across agency boundaries, the provider shall be held accountable to protect and share audit information with the agency through the contract. [AU-16]

6. AUDIT REVIEW, ANALYSIS, AND REPORTING

6.1. Daily Log Review:

6.1.1. Daily log reviews shall at a minimum include those entries that have been deemed most likely to be important, as well as some of the entries that are not yet fully understood. [AU-6]

6.1.2. Items for daily log review checks [AU-6]:

- Error and Warning events from server logs
- All logged events from domain controller security logs
- All logged events from firewall and web server security logs
- SYSLOG devices, severity error codes 0 thru 4

6.2. Weekly Log Review:

6.2.1 Weekly log reviews shall at a minimum include events not requiring immediate action from daily reviews.

6.2.2. Items for weekly log review checks [AU-6]:

- All access audit logs
- Error and Warning events from workstation logs
- All logged events from file and application servers (other than firewall and web server)
- Application logs (e.g., Exchange, IIS, ISA Server, FTP Server)
- SYSLOG devices, severity error codes 5 thru 6

6.3. Log Data Access [AC-5]:

6.3.1. Authorized system, network, and security administrators may be granted access to system log files if they have a valid need to know.

- 6.3.2. Agency executive management may grant personnel access to agency specific log files.
- 6.3.3. Authorized information system auditors may have access to log files when performing audit duties.
- 6.3.4. Incident response personnel may have access to log data when necessary to handle security incidents.

6.4. Reporting:

- 6.4.1. Patterns indicating unauthorized, suspicious, or illegal behavior shall be brought to the attention of appropriate management and an action plan determined. Immediate action shall be taken on events identified as critical to network/system performance/function or events that may reflect unauthorized or illegal activity. Events not requiring immediate action will be identified and scheduled for review. [AU-6]
- 6.4.2. Unauthorized disclosure of sensitive information recorded in logs, such as personally identifiable information (PII), shall be reported to the Senior Agency Information Security Officer or Privacy Officer and handled as a cybersecurity incident. [IR-6]

7. ADDITIONAL AUDIT REQUIREMENTS FOR MODERATE OR HIGH-RISK SYSTEMS:

For moderate or high-risk systems (systems which process, transmit, or store sensitive or confidential information or systems that require additional audit safeguards as determined by a risk assessment) the following additional requirements shall be applied:

- 7.1. Agencies shall review and update the audited events at a minimum, annually. [AU-2 (CE3)]
- 7.2. Audit Content: Additional information that should be included in audit records if available for capture from information systems include layer 2 through 4 of the OSI model (source and destination IP and MAC address and TCP/UDP ports). [AU-3 (CE1)]
- 7.3. Process Integration: Organizations shall employ automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities. [AU-6 (CE1)]
- 7.4. Automatic Processing: Information systems shall provide the capability to process audit records for events of interest based on selectable event criteria. [AU-7 (CE1)]

7.5. Time Stamps:

7.5.1. Information systems shall compare their system clock to one or more of the following federally-managed NTP (Network Time Protocol) servers:

- NIST Internet Time Servers
- US Naval Observatory NTP Servers [AU-8 (CE1(a))]

7.5.2. Information systems shall be configured to compare the internal system clock to the time source at least once daily and when the system is booted. [AU-8 (CE1(a))]

7.5.3. Internal system clocks shall be synchronized to the time source when the time difference is greater than 0.1 seconds (or one hundred milliseconds). [AU-8 (CE1(b))]

7.6. Restrict access to manage audit functionality only to designated security administrators. System and network administrators shall not have the ability to modify or delete audit log entries. [AU-9 (CE4)]

SUPPORTING DOCUMENTS

The following documents support this standard:

- [Policy 645: Audit and Accountability](#)

The following special publication (SP) of the National Institute of Standards and Technology (NIST) supports these requirements and may aid in their implementation:

- NIST SP 800-92: Guide to Computer Security Log Management

EFFECTIVE DATE

This standard is effective upon its approval by the Secretary of Information Technology, as evidenced by the signature of the Secretary being affixed hereto.

The undersigned, as Secretary of Information Technology of the State of Alabama, exercising the power vested in that Office by the laws of this state, declares this standard to be adopted as of the _____ day of _____, 2020.

Marty Redden
Secretary of Information Technology

DOCUMENT CHANGE HISTORY

Version	Version Date	Comments
645S1-01	07/09/2020	Initial version (draft); supersedes Standard 677S1: Log Management

DRAFT