State of Maryland

STANDARD

AUDIT & ACCOUNTABILITY

Document No.	Last Updated	Prepared By
MD-STD-303-AU-01	02/18/2026	DOIT OSM

Audit and accountability are fundamental components of Zero Trust Architecture (ZTA), enabling continuous monitoring, real-time logging, automated anomaly detection, and the ability to track system activity and detect unauthorized access.

PURPOSE AND SCOPE

Purpose	This standard requires systems to generate, protect, and retain audit records to support the detection, investigation, and response to unauthorized or suspicious activity.
Scope	This standard covers all IT assets with logging capabilities and is not specific to any single platform or technology solution.
Applicability	This standard applies to all units of State government (as defined in SF&P 3.5-101(g)), hereafter referred to simply as "agencies."
Related Policy	This standard is part of a broader policy suite. Refer to MD-POL-100 Cybersecurity & Governance Policy, Appendix C for a list of related policies and standards.
Baseline	This standard has been developed using National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 5 Moderate Baseline[1] and State-specific organizationally defined parameters. Agencies may be required to deviate from this baseline when State statute, executive orders, or applicable regulations establish a conflicting requirement that precludes compliance.
Distribution	This standard is approved for public distribution and may be shared with external stakeholders, partners, and regulatory bodies. It reflects the State's commitment to transparency, compliance, and operational excellence. Unauthorized modifications or misrepresentation of this document are strictly prohibited.

[1] NIST SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations.

FOREWORD

Agencies that use Department of Information Technology DoIT-managed services automatically receive, or *inherit*, the compliance those services already meet, reducing duplicative work and accelerating their overall compliance efforts. These centrally governed services, such as hosting platforms, identity management, and network infrastructure, are built with robust control frameworks that automatically extend to participating agencies. By leveraging these offerings, agencies not only align with key operational and security standards but also benefit from pre-configured environments, continuous monitoring, and policy enforcement mechanisms maintained by DoIT. Agencies are encouraged to leverage these services to accelerate readiness, gain cost efficiency, simplify compliance efforts, and allow agencies to focus more fully on mission delivery, knowing that foundational requirements are already in place. Agencies should review the scope of each managed service to understand which standards are inherited and where additional agency-specific controls may still be required.

GUIDANCE AND ENFORCEABILITY

Throughout this document, informational call-out boxes are utilized to provide additional context or elaborate on key topics. While these boxes primarily serve an informational purpose, any directives or mandated actions contained within them are authoritative and carry the same enforceability as the core requirements of this document. For the purposes of this document, the term “shall” denotes a mandatory requirement. Terms such as “where feasible”, “encouraged”, or similar phrasing indicate recommended practices that reflect organizational preference but are not enforceable requirements at this time.

CHANGE RECORD

Version	Summary of Changes	Changed By	Date
1.0	Initial Publication	Miheer Khona	02/18/2026

STANDARDS

303 State Strategy

These standards establish a baseline of audit and accountability practices that each agency must implement to comply with State cybersecurity and privacy policies. Each agency shall designate specific personnel with IT responsibilities to ensure the effective implementation of these standards.

303-1 Develop Agency-Level Procedures (AU-1)

In alignment with this standard, develop and document agency-level audit and accountability procedures for systems and applications. Agencies must disseminate the procedures to agency personnel with information technology (IT) security responsibilities. Agencies must review, and if needed, update the procedures as deemed appropriate by the agency based on changes and risk at least every **3 years**. At a minimum, the procedures must address purpose, scope, roles and responsibilities, and guidelines.

303-2 Identify Auditable Events (AU-2)

Identify the types of events that the system is capable of logging in support of the audit function. The types of events that can be logged vary by system. 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.

Specify the event types for logging within the system along with the frequency of (or situation requiring) logging for each identified event type and provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents. Review and update the event types selected for logging at least **annually**. Agencies shall document event selection rationale in the System Security Plan (SSP).

Audit-Relevant Telemetry Sources (Non-exhaustive examples)

Technology Type	Technology Type
Identity, Credential, and Access Management	Secure Web Gateway or Domain Name System (DNS) Proxy
Endpoint Logs (Servers, Workstations, Laptops)	Cyberthreat Intelligence (CTI)
Network Device Infrastructure Logs	Privileged Access Management (PAM)
Cloud Environment Logs	Virtual Desktop Interface (VDI)
Amazon Web Service Events	Data Loss Prevention (DLP) for Email, Cloud Drives, and Endpoints
Microsoft Azure Cloud	Cloud Access Security Broker (CASB)
Azure Active Directory Logs, Azure Activity	Configuration Management Database (CMDB)

Technology Type	Technology Type
Google Cloud Logs	Hardware & Endpoint Inventory
Email Logs	Business Service, Application, and System Inventories
Additional Network Logs	Critical Business Applications
Web Application Server	Software Inventory
Mobile Device Logs	Vulnerability Scan Reports

303-3 Determine Content of Audit of Records (AU-3)

Configure audit records to contain information that establishes the following:

- What type of event occurred;
- When the event occurred;
- Where the event occurred;
- Source of the event;
- User ID (if available), but do not log password used;
- Action/request attempted (e.g., interface status changes, changes to the system configuration, access list matches and/or failures);
- Outcome of the event; and
- Identity of any individuals, subjects, or objects/entities associated with the event.

AU-3(1): Generate audit records, when system functionality permits, that includes additional audit detail that may assist in incident investigations such as full text recording of privileged commands, and the individual identities of group account users.

303-4 Allocate Audit Log Storage Capacity (AU-4)

Allocate sufficient audit log storage capacity to reduce the likelihood of such capacity being exceeded and resulting in the potential loss or reduction of audit logging capability.

Calculating Audit Storage Needs

To determine audit log storage capacity effectively, especially in hybrid environments, agencies must blend technical telemetry modeling with compliance-driven retention planning. To calculate the capacity needs: a) Define audit scope and sources; b) Estimate log volume per source; c) Define retention requirements; d) Calculate total storage need; and e) Plan for storage management.

303-5 Respond to Audit Logging Process Failures (AU-5)

Alert designated agency officials (in the agency defined period) in the event of audit failure, unusual or inappropriate audit activity, or audit storage capacity being reached.

Take the following actions:

- Shut down, overwrite the oldest records, or cease information system processing;
- Document justification in the SSP; and
- Provide a warning when allocated audit record storage volume reaches a maximum audit record storage capacity.

303-6 Perform Audit Record Review, Analysis, and Reporting (AU-6)

Perform Audit Record Review, Analysis, and Reporting by:

- Review and analyze in near real time or at minimum weekly, based on system criticality and risk, for indications of inappropriate or unusual activity;
- Define inappropriate or unusual activities in the SSP for each system;
- Report findings to agency designated officials including incident response team and (if necessary) escalate to the State Chief Information Security Officer (SCISO);
- Adjust the level of audit 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; and
- Perform automated analysis across user and entity activity log types and augment collection to address gaps in visibility.

All information systems connected to a Maryland State network shall utilize the DoIT approved centralized audit record management solution with the requirements defined by the SCISO and the program manager for the enterprise-wide auditing solution. Agencies will be provided with access, as needed, to the enterprise solution for monitoring agency alerts. Any deviations due to the functionality, operational requirements, or capabilities of a system which is not utilizing the central logging system for audit review, analysis, and reporting process, must be clearly defined and justified in the SSP. Compensating security controls shall be clearly documented to meet security control requirements.

AU-6(1): Integrate audit record review, analysis, and reporting processes using automated mechanisms.

AU-6(3): Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.

303-7 Implement Audit Record Reduction and Report Generation (AU-7)

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

Any information system that is not capable of providing logs to the DoIT enterprise audit generation tools due to system functionality and operational requirements must be documented in its SSP, the process by which its logs may be sorted and organized for more meaningful analysis.

AU-7(1): Information systems must provide the capability to automatically process, sort and search audit records for events of interest based upon selectable event criteria including but not limited to: identities of individuals, event type, event dates, event location, Internet Protocol (IP) address involved, information objects, or system resources involved.

303-8 Generate Time Stamps (AU-8)

Use internal system clocks to generate time stamps for audit records; and record time stamps for audit records that meet the **5 second offset** requirement[2] and that use Coordinated Universal Time (UTC), have a fixed local time offset from UTC, or that include the local time offset as part of the time stamp.

303-9 Protect Audit Information (AU-9)

Protect audit information and audit logging tools from unauthorized access, modification, and deletion. Restrict audit trails from being read or modified by non-administrator users. System and network administrators shall not have access to audit logging management functions unless explicitly authorized; and alert agency designated personnel upon detection of unauthorized access, modification, or deletion of audit information.

AU-9(4): Authorize access to management of audit logging functionality to only authorized security administrators as documented in the SSP. Restrict audit trails from being read or modified by non-administrator users, and system and network administrators.

Zero Trust Architecture

Privileged access should be further defined between audit related privileges and other privileges, thus limiting access to those users with audit-related privileges. To preserve the integrity and objectivity of the auditing and network monitoring functions, segregation of duties must be maintained. No single individual may have control over all phases of audit functionality and network monitoring.

[2] In cybersecurity and IT operations, a "5-second offset" refers to the maximum allowable time difference between system clocks.

303-10 Retain Audit Records (AU-11)

Retain online audit records for the duration required by State record retention laws and applicable regulations (e.g., MD State Archives, HIPAA) to provide support for after-the-fact investigations of incidents.

303-11 Audit Record Generation (AU-12)

Provide audit record generation capability for the event types the system is capable of auditing. Allow agency designated personnel to select the event types that are to be logged by specific components of the system; and generate audit records.

GUIDELINES

ID	Title	Description	Source
CSF Tools	Cyber security Framework Tools	This website provides supplemental guidance for each security control listed in this document.	*csf.tools (LINK)*
NIST SP 800-93	Guide to Computer Security Log Management	This document provides detailed guidance on managing audit logs effectively. It covers best practices for log collection, storage, analysis, and protection to support security monitoring and compliance.	*csf.tools (LINK)*

DEFINITIONS

Each unique term used in this standard is defined in the **State of Maryland Cybersecurity & Privacy Glossary**.

COMPLIANCE CHECKLIST

ID	Standard	Compliance
303-1	**Develop Agency-Level Procedures (AU-1)**	☐ Yes ☐ No
303-2	**Identify Auditable Events (AU-2)**	☐ Yes ☐ No
303-3	**Determine Content of Audit of Records (AU-3)**	☐ Yes ☐ No
303-4	**Allocate Audit Log Storage Capacity (AU-4)**	☐ Yes ☐ No
303-5	**Respond to Audit Logging Process Failures (AU-5)**	☐ Yes ☐ No
303-6	**Perform Audit Record Review, Analysis, and Reporting (AU-6)**	☐ Yes ☐ No
303-7	**Implement Audit Record Reduction and Report Generation (AU-7)**	☐ Yes ☐ No
303-8	**Generate Time Stamps (AU-8)**	☐ Yes ☐ No
303-9	**Protect Audit Information (AU-9)**	☐ Yes ☐ No
303-10	**Retain Audit Records (AU-11)**	☐ Yes ☐ No
303-11	**Audit Record Generation (AU-12)**	☐ Yes ☐ No

Note: When assessing the implementation and effectiveness of the security and privacy controls outlined in this standard, DoIT recommends the use of NIST SP 800-53A Rev. 5, to perform evaluations in a manner that is evidence-based, repeatable, and aligned with the system's documented security posture.