State of Maryland

STANDARD

CONTROL ASSESSMENTS

Document No.	Last Updated	Prepared By
MD-STD-304-CA-01	02/18/2026	DOIT OSM

Within a Zero Trust Architecture (ZTA), information systems must undergo regular security evaluations, receive formal authorization before operation, and be continuously monitored through ongoing risk assessment, adaptive access controls, and real-time threat detection.

PURPOSE AND SCOPE

Purpose	This standard establishes a process for each agency to systematically evaluate the security posture, authorize systems before deployment, and continually monitor for risk.
Scope	This standard provides an organizational approach for assessment, authorization, and monitoring 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 document 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

304 State Strategy

These standards establish a baseline of control assessment 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. These standards do not address the additional assessment requirements that may be required by external audit agencies and should be addressed as a supplement to these standards.

304-1 Develop Agency-Level Procedures (CA-1)

In alignment with this standard, develop and document agency-level assessment, authorization, and monitoring procedures. 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.

304-2 Perform Control Assessments (CA-2)

Select the appropriate assessor or assessment team for the type of assessment to be conducted and develop a control assessment plan that describes the scope of the assessment including:

- Controls and control enhancements under assessment;
- Assessment procedures to be used to determine control effectiveness; and
- Assessment environment, assessment team, and assessment roles and responsibilities.

Review the control assessment plan and gain approval by the appropriate Authorizing Official (AO) prior to conducting the assessment.

Produce a control assessment report that documents the results of the assessment and provide the report to the appropriate AO.

Assessment Report Sources

Agencies can draw from several sources, provided the sources are current and relevant to determining security control effectiveness. These sources include but are not limited to: a) Assessments conducted as part of the information system authorization or re-authorization process; b) Continuous monitoring activities; and c) Testing and evaluation of information systems as part of the ongoing system development lifecycle (SDLC) process.

CA-2(1): Employ independent assessors or assessment teams to conduct control assessments using the following guidelines:

- Independent assessors can be Information Security Officers (ISO) obtained from within the DoIT Office of Security Management (OSM) or can be contracted to public or private sector entities.
- Authorizing officials shall consult the State Chief Information Security Officer (SCISO) when determining the required level of assessor independence.

Assessor Independence

Assessors must maintain a degree of independence and impartiality that is free from perceived or actual conflicts of interest with respect to the determination of control effectiveness or the development, operation, or management of the system, common controls, or program management controls. At a minimum, selected assessors shall: a) Not have conflicting interests with the agency; b) Not evaluate their own work; c) Not be under the supervision of the department being assessed; and d) Not advocate for the agency acquiring their services.

304-3 Manage Information Exchanges (CA-3)

Approve and manage the exchange of information between the system and other systems using formal exchange agreements (e.g., interconnection security agreements; information exchange security agreements; memoranda of understanding or agreement; service level agreements; data use agreements (for the exchange of personally identifiable information); data sharing agreements (with intra-State agencies), nondisclosure agreements).

Document, as part of each exchange agreement, the interface characteristics, security and privacy requirements, controls, and responsibilities for each system, and the impact level of the information communicated and review and update the agreements **annually** or as otherwise indicated in each exchange agreement.

Common Information Exchanges

The State routinely exchanges information across agencies and jurisdictions. Examples of information exchanges that necessitate an agreement in place include but are not limited to: a) Leased lines or virtual private networks (VPN); b) Internet Service Providers; c) Database sharing and transaction exchanges; d) Cloud services; e) Web-based services; f) File transfers (e.g., SFTP, IPv4, IPv6, email); and g) Agency-to-agency communications.

304-4 Maintain Plans of Action and Milestones (CA-5)

Develop a system plan of action and milestones (POA&M) to document the planned remediation actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system; and update existing POA&Ms at least **monthly** based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities.

304-5 Explicitly Authorize Systems for Operation (CA-6)

Assign a senior official as the AO for the system and for common controls available for inheritance by organizational systems.

Before commencing operations, the AO for the system must:

- Review the use of common controls inherited by the system for acceptability; and
- Authorize the system to operate as deemed appropriate based on risk.

Agency AOs shall perform expedited assessments, within the timeframe set by DoIT OSM, for prioritized subsets of controls when requested.

Update the security authorizations every **3 years** or upon significant change to the system that may require reauthorization. Where continuous monitoring is fully implemented and approved by the AO, reauthorization frequency may be extended to every **5 years**. For systems deemed a High Valued State System (HVSS), reauthorization may be required more frequently as defined by the SCISO, commensurate with risk.

304-6 Conduct Continuous Monitoring (CA-7)

Develop a system-level continuous monitoring strategy and implement monitoring in accordance with the organization-level continuous monitoring strategy to include:

- System-level metrics to be monitored (i.e., Number of controls met, unmet, partially met; and number of open vulnerabilities by risk rating);

- Continuous monitoring activities including periodic reauthorization (per section 304.5), security impact analysis for changes, annual review of security controls, quarterly vulnerability scans, and risk assessments regarding system vulnerabilities;
- Correlation and analysis of information generated by control assessments and monitoring;
- Response actions to address results of the analysis of control assessment and monitoring information; and
- Reporting the security and privacy status of the system to appropriate agency executives, AO (or delegate) and DoIT officials (e.g., SCISO, State Chief Privacy Officer (SCPO), State Chief Data Officer (SCDO) annually.

CA-7(1): The agency shall monitor the security controls in the information system on an ongoing basis using either an internal assessor or external independent assessor.

CA-7(4): The agency shall monitor risk as part of the continuous monitoring strategy to include monitoring for effectiveness, compliance, and changes.

304-7 Explicitly Authorize Internal System Connections (CA-9)

Authorize internal connections to the system and document, for each internal connection, the interface characteristics, security and privacy requirements, and the nature of the information communicated.

Terminate internal system connections after the minimum time tolerance defined by the IT manager and approved by the AO. Following ZTA principles, review the need for each internal connection at least **quarterly**, and more frequently where feasible.

Authorizing System Connections
While there are numerous authorization mechanisms that can be used to explicitly authorize internal system connections, the following three steps provide an efficient approach that align to the broader set of State policy, standards, and risk management strategy: a) Document the connection purpose in the System Security Plan (SSP); b) Perform a risk assessment as part of the MD State Authorization to Operate (ATO) process; and c) Establish authorization via a signed ATO and supporting SSP.

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 800-53A	Assessing Security and Privacy Controls in Information Systems and Organizations	This document provides a structured approach to assessing security and privacy controls.	*csrc.nist.gov (LINK)*
NIST SP 800-137	Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations	This document provides guidance on developing a continuous monitoring strategy to maintain visibility into organizational assets, threats, vulnerabilities, and the effectiveness of security controls.	*csrc.nist.gov (LINK)*
NIST SP 800-37	Risk Management Framework for Information Systems and Organizations	This document defines the RMF process, including security authorization and ATO procedures.	*csrc.nist.gov (LINK)*
NIST Privacy Framework	NIST Privacy Framework	This document helps organizations to identify and manage privacy risk.	*nist.gov (LINK)*

DEFINITIONS

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

COMPLIANCE CHECKLIST

ID	Standard	Compliance
304-1	**Develop Agency-Level Procedures (CA-1)**	☐ Yes ☐ No
304-2	**Perform Control Assessments (CA-2)**	☐ Yes ☐ No
303-3	**Manage Information Exchanges (CA-3)**	☐ Yes ☐ No
303-4	**Maintain Plans of Action and Milestones (CA-5)**	☐ Yes ☐ No
303-5	**Explicitly Authorize Systems for Operation (CA-6)**	☐ Yes ☐ No
303-6	**Conduct Continuous Monitoring (CA-7)**	☐ Yes ☐ No
303-7	**Explicitly Authorize Internal System Connections (CA-9)**	☐ 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.