## State of California

## Department of Technology

# Zero Trust Architecture Standard

**Statewide Information Management Manual – 5350-A**

**September 2025**

# Table of Contents

## Document History

| Revision | Date of Release | Owner | Summary of Changes |
|---|---|---|---|
| v.1 | September 2025 | Office of Information Security (OIS) | Initial release |

# Introduction

## Purpose

Zero Trust Architecture (ZTA) is crucial for state governments to ensure digital trust, by continuously validating every user, service, and device, by default, whether inside or outside a network, reducing the risk of data breaches and cyberattacks. Instead of relying on traditional perimeter-based security approaches that assume everything inside the network is trustworthy, Zero Trust assumes that threats could be both external and internal. It requires strict verification and validation for all users, devices, and network components attempting to access resources.

This standard provides a phased approach to implementing ZTA, building upon State Administrative Manual (SAM) 5350. State agencies and entities are required to adopt the security controls listed in SIMM 5350-B.

## Scope

This standard applies to all California state entities, including agencies, departments, divisions, bureaus, boards, and commissions, as defined in Gov Code Section 11546.1.

## Compliance

As outlined in Government Code (GC) Section 11549.3, the Office of Information Security (OIS) is entrusted with creating, issuing, and maintaining policies, standards, and procedures, overseeing information security risk management for agencies and state entities, providing information security and privacy guidance, and ensuring compliance with State Administrative Manual (SAM) Chapter 5300 and Statewide Information Management Manual (SIMM) section 5300.

State entities must adhere to OIS-issued information security and privacy policies, as well as all relevant governing laws, regulations, rules, and standards. Compliance may be reflected in audit findings and maturity scores. Non-compliance will be addressed according to the Office of Information Security Policy Compliance and Enforcement Standard (SIMM 5330-H).

**Definitions**

**Zero Trust Architecture**: A security trust model that assumes that no entity should be inherently trusted, whether internal or external. It requires strict verification and authentication for users, devices, and applications seeking access to resources.

## Zero Trust Tenets

ZTA uses Zero Trust tenets to plan industrial and enterprise infrastructure and workflows. The Cybersecurity & Infrastructure Security Agency's (CISA) Zero Trust Maturity Model documentation describes five ZTA pillars as the foundational layers to adopt ZTA. These are: Identity, Devices, Networks, Applications and Workloads, and Data. Each pillar can progress at its own pace and may progress more quickly than others until cross-pillar coordination is required. The model is designed to augment adherence to Zero Trust tenets listed in the National Institute for Standards and Technology's (NIST) SP 800-207:

1. All data sources and computing services are considered resources.
2. All communication is secured regardless of network location.
3. Access to individual enterprise resources is granted on a per-session basis.
4. Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes.
5. The enterprise monitors and measures the integrity and security posture of all owned and associated assets.
6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed.
7. The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.

## Architecture Controls

Agency/State entities are required to establish the security and privacy controls outlined in NIST SP 800-53 Rev 5, as detailed in Appendix-A in SIMM 5350-B pertaining to the applicable ZTA components.

Agency/State entities shall adopt a ZTA that is implemented in a phased, risk-based manner. This shall begin with a comprehensive inventory of assets and the development of access policies based on least-privilege and observed access patterns. Existing security capabilities shall be evaluated for integration into the ZTA framework. Implementation shall prioritize core components such as identity verification and device health assessments, with ongoing monitoring and periodic reassessment to ensure continuous alignment with evolving threats, technologies, and mission requirements. Zero Trust shall be maintained as a continuous improvement lifecycle.

Agency/State entities are to consistently enhance their security posture by adopting the established State Baseline Maturity (Levels 1 and 2) and subsequently progress their ZTA maturity to the Optimized Maturity (Levels 3 and 4) where and when applicable.

Table 1 shows the State Baseline and Optimized requirements by Maturity Level that entities should progress towards. **The inability to implement a required SIMM 5350-B ZTA security control for any system must be recorded as a risk in the Risk Register and Plan of Action Milestones (SIMM 5305-C).**

| | Maturity Level | Description |
|---|---|---|
| State Baseline | Level 1 Traditional | Manually managed lifecycles with assigned security attributes; rigid security policies addressing isolated pillars reliant on external systems; least privilege enforced only at setup; fragmented policy enforcement; manual threat response; and weak correlation of dependencies, logs, and telemetry. |
| | Level 2 Initial | Automating attribute assignment, lifecycle configuration, and policy enforcement; integrating external systems for cross-pillar solutions; adjusting least privilege post-provisioning; and enhancing internal visibility. |
| Optimized | Level 3 Advanced | Automated lifecycle and policy controls with cross-pillar coordination; centralized visibility and identity management; integrated enforcement; predefined mitigation responses; risk-based privilege adjustments; and enterprise-wide awareness, including external resources. |
| | Level 4 Optimal | Fully automated, just-in-time lifecycles and attribute assignments; self-reporting assets with dynamic, trigger-based policies; adaptive least privilege access across dependencies; cross-pillar interoperability with continuous monitoring; and centralized visibility for situational awareness. |

***Table 1: ZTA Maturity Levels and their description***

## Tracking Progress

State entities must continuously assess, document, and report their progress in implementing ZTA principles. They are responsible for tracking completed security measures, identifying outstanding risks, evaluating their impact, and documenting gaps where ZTA is not applicable or feasible. Additionally, entities must maintain a structured implementation plan to address security gaps and advance ZTA planned adoption. Key areas of focus in the implementation plan shall include authentication, trusted networks, enforcing least privilege principles, restricting lateral cyber threat movement, and enhancing the rapid detection, isolation, and removal of unauthorized users and devices.

Table 2 outlines the NIST Cybersecurity Framework (CSF) 2.0 categories relevant to a ZTA environment. The detailed mapping of CSF 2.0 objectives is highlighted in SIMM 5350-B – Supplemental CSF Mapping tab.

| Function | Category | |
|---|---|---|
| GOVERN | GV.OC<br>GV.RM<br>GV.RR<br>GV.PO<br>GV.SC | Organizational Context<br>Risk Management Strategy<br>Roles, Responsibilities, and Authorities<br>Policy<br>Cybersecurity Supply Chain Risk Management |
| IDENTIFY | ID.AM<br>ID.RA<br>ID.IM | Asset Management<br>Risk Assessment<br>Improvement |
| PROTECT | PR.AA<br>PR.DS<br>PR.PS<br>PR.IR | Identity Management, Authentication, and Access Control<br>Data Security<br>Platform Security<br>Technology Infrastructure Resilience |
| DETECT | DE.CM<br>DE.AE | Continuous Monitoring<br>Adverse Event Analysis |
| RESPOND | RS.MA<br>RS.AN<br>RS.MI | Incident Management<br>Incident Analysis<br>Incident Mitigation |
| RECOVER | N/A | |

*Table 2: NIST CSF 2.0 categories relevant to a ZTA environment*

## Resources

SIMM 5350-B contains resources that identify the ZTA technical requirements. The Appendix-A tab maps the functions provided by the logical components of the ZTA reference design and NIST SP 800-53 security controls. Supplemental CSF Mapping tab maps the functions of the ZTA reference design components and the NIST CSF 2.0 functions.

## References

- **CISA Zero Trust Maturity Model**
  https://www.cisa.gov/zero-trust-maturity-model
- **DoD Zero Trust Strategy**
  https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf
- **NIST SP 800-207 – Zero Trust Architecture**
  https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf
- **NIST SP 1800-35 – Implementing a Zero Trust Architecture**
  https://csrc.nist.gov/pubs/sp/1800/35/final
- **NIST Cybersecurity Framework 2.0**
  https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-csf-20/final
- **NIST Security and Privacy Controls Rev5**
  https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final
- **SAM 5350 Operational Security**
  https://www.dgs.ca.gov/Resources/SAM/TOC/5300/5350
- **SAM 4983.1 Cloud Computing Policy**
  https://www.dgs.ca.gov/Resources/SAM/TOC/4900/4983-1
- **SIMM 140 Cloud Security Guide**
  https://cdt.ca.gov/wp-content/uploads/2023/10/SIMM-140-Cloud-Security-Guide-1.docx
- **SIMM 5305-A Information Security Program Management Standard**
  https://cdt.ca.gov/wp-content/uploads/2023/12/SIMM-5305_A_2023-12.pdf
- **US Government Accountability Office GAO-23-106065 Zero Trust Architecture**
  https://www.gao.gov/assets/gao-23-106065.pdf

## Questions

Questions regarding the implementation of this standard may be sent to:

California Department of Technology

Office of Information Security Security@state.ca.gov