State of California
Department of Technology
Office of Information Security
Information Security Policy Compliance and Enforcement Standard
SIMM 5330-H

November 2024

Revision History

REVISION	DATE OF RELEASE	OWNER	SUMMARY OF CHANGES
v.1	November 2024	Office of Information Security	Initial release

Purpose

Information security governance is vital to managing and mitigating information security and privacy risk. It involves several critical components, including, but not limited to, defining organizational priorities and risk thresholds, evaluating risk, establishing comprehensive policies and procedures, and clarifying roles and responsibilities related to information security.

This Standard supports State Administrative Manual (SAM) 5300 by establishing information security compliance and an enforcement protocol. Governance is included in the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0. The NIST Governance function guides organizations in implementing the remaining five functions: identification, protection, detection, response, and recovery.

Applicability

This standard applies to all California state entities, including agencies, departments, divisions, bureaus, boards, and commissions, as defined in Government Code (GC) Section 11546.1, responsible for information security activities.

Scope

This standard outlines how the Office of Information Security (OIS) exercises its oversight responsibilities and the consequences of non-compliance with information security and privacy policies, standards, and procedures established by OIS.

OIS Oversight

I. Compliance Assessments

Compliance standards exist to ensure state entities adhere to statewide policies, procedures, and standards.

GC Section 11549.3 authorizes OIS to create, issue, and maintain policies, standards, and procedures.

Additionally, it oversees information security risk management for state entities, provides information security and privacy guidance, and ensures 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 and all relevant laws, regulations, rules, and governing standards. Full compliance is expected, and noncompliance will be addressed according to this standard and associated procedures.

OIS assesses compliance through a variety of sources, including but not limited to:

- Internal & External Assessments
    - Including Independent Security Assessments (ISA)
- Internal & External Audits
- Asset Scanning Vulnerability Reports
- Compliance Reviews
- Self-Assessments
- Asset Assessments
- Risk Assessments
- Entries in the Risk Register and Plan of Action and Milestones (RRPOAM)
- System Security Plans as required in the California Compliance and Security Incident Reporting System (Cal-CSIRS)

II. Enforcement Protocol

Ensuring compliance with OIS policies, standards, processes, and procedures is crucial for maintaining a safe and secure working environment. Should there be instances of non-compliance with policies, standards, processes, and procedures, including overlooked risk mitigation or remediation efforts, OIS may intervene to guide compliance and risk mitigation efforts.

The Enforcement Protocol includes three phases: Preventative, Corrective, and Adverse. Repeated non-compliance with policies, procedures, and standards may result in a direct escalation to the Adverse phase.

i. Preventative Phase

In the Preventative phase, OIS will consult with the affected entity, document compliance findings, and provide support and guidance for remediation.

This consultation facilitates the development of an initial corrective action plan tailored to the entity's needs. The plan defines the timeline and actions that must be taken to demonstrate compliance.

The entity must also include the non-compliant issue or risk in their Risk Register/Plan of Action and Milestones (RRPOAM) and select ‘Corrective Action Plan’ as the source of the finding. Corrective Action Plan entries must align with SAM and SIMM policies and standards.

ii. Corrective Phase

The Corrective phase is initiated if the entity fails to demonstrate progress towards compliance according to the timeline identified in the initial action plan or if the state's Chief Information Security Officer (CISO) determines that a risk is too great for the state of California and requires immediate action.

During this phase, OIS will establish formal requirements for addressing compliance and risk findings. Non-compliance may be escalated through the Notification Protocol, and enrollment in mandatory information security risk mitigation services may be required.

iii. Adverse Phase

If the Corrective phase does not result in compliance, OIS may initiate the Adverse phase. This involves enforcement actions such as reducing, suspending, or terminating administrative delegations and increasing information security compliance monitoring activities. The entity will receive a 30-day advance notice of the enforcement action that will be taken, including the duration and necessary steps to clear the enforcement action. Each enforcement action and its remediation steps will be on a case-by-case basis, and communications will be sent according to the Notification Protocol.

III. Enforcement Actions

Enforcement actions may influence administrative functions. Examples of administrative functions that may be impacted include, but are not limited to:

- Budget Change Proposal (BCP) Submissions

    - Lack of information security maturity may influence recommendations provided on funding proposals.
- Cloud Computing Exemptions and Authorization to Operate
    - Lack of information security maturity may impact the determination of whether an entity may operate a cloud hosted environment.
- IT Procurement and Project Cost Delegation for Reporting
    - Lack of information security maturity may affect project cost delegation and require increased oversight of technology projects and procurements.
- Compliance Reporting Frequency
    - Lack of information security maturity may increase the frequency of self-reported compliance documentation or additional reporting requirements.
- Information Security Program Audit (ISPA) and Independent Security Assessment (ISA) frequency.
    - Lack of information security maturity may increase the frequency of oversight agency engagements.
- Mandatory Information Security Risk Mitigation Services
    - Lack of information security maturity may lead to enrollment in mandatory risk mitigation services and billed via a monthly rate.

Correcting compliance failures will reinstate administrative functions, with potential audits and assessments to confirm remediation effectiveness.

IV. Communication and Notification Protocol

OIS will initiate communication with entities throughout each phase based on their most recent SIMM 5330-A Designation letter. Secure electronic communication will be used to document each notification. Verbal conversations will be followed with a written summary and distributed to all participants to provide a record of the communication.

i. Communication Protocol

A communication protocol is essential in maintaining effective communication by ensuring that conversations do not stagnate or remain unresolved. This protocol involves a systematic approach where participants are encouraged to respond and engage within a specified timeframe, keeping the dialogue active and progressive.

	Compliance Communication Sent From OIS	Entity Acknowledgement of Communication	Entity Response to Communication
1	Initial Contact	Within 5 business days of initial contact	Within 10 business days of the last acknowledgment
2	Correspondence	Within 5 business days of the last communication	Within 10 business days of the last acknowledgment

If OIS does not receive timely responses from the entity and further follow-ups are required, reminders will be issued with requests to acknowledge or reply to the most recent correspondence. Periods of nonresponse will begin after the deadlines set for initial replies have elapsed.

	Communication Nonresponses	Entity Acknowledgement	Entity Response
1	First follow-up communication	Within 3 business days of the first follow-up	Within 7 business days of the last acknowledgment
2	Second follow-up communication	Within 2 business days of the second follow-up	Within 5 business days of the last acknowledgment
3	Final notice	Within 1 business day of the final notice	Within 2 business days of the last acknowledgment

Once communication is re-established, the communication protocol will revert to the standard 5/10 business days for acknowledgments and responses. Nonresponses and missed deadlines will escalate through the Notification Protocol timeline.

ii. Notification Protocol

A notification protocol is crucial when communication becomes stagnant, particularly when noncompliance issues that require urgent resolution are identified. This protocol ensures that if initial communications fail to produce the necessary response or action, the matter is promptly escalated to higher levels of authority to prioritize the issue, ensuring it receives the appropriate attention and intervention.

Communication From	Communication To	Escalation To
State Risk Program Manager or delegate.	Information Security Officer (ISO) or delegate.	State Security Risk Governance Chief or delegate.
State Security Risk Governance Chief or delegate.	Department Chief Information Officer (CIO) or delegate.	State Chief Information Officer and Deputy State Information Officer. Agency/state entity Director or delegate. Agency Information Security Officer (AISO) or delegate.
State Security Risk Governance Chief or delegate. Agency Information Security Officer (AISO) or delegate.	Entity Director or delegate.	Agency Information Officer (AIO) or delegate. State Chief Information Security Officer (CISO) and State Deputy CISO or delegate.
State Chief Information Security Officer (CISO) and State Deputy CISO or delegate.	Agency Information Officer (AIO) or delegate.	State Chief Information Officer (CIO) and State Deputy CIO or delegate.
State Chief Information Security Officer (CISO) and State Deputy CISO or delegate. State Chief Information Officer (CIO) and State Deputy CIO or delegate.	Agency Information Officer (AIO) or delegate.	Agency Secretary's Office or delegate. Cal-CSIC Executive Partners.
GovOps Secretary's Office or delegate.	Governor's Office (the Governor) or delegate.	

V. Extensions

During the Corrective phase, entities collaborate with OIS. If entities need more time to comply with the established timelines, they can submit their extension requests through the OIS delegate they have been coordinating with. This established working relationship helps to streamline the process of requesting and reviewing time extensions, analyzing risks, and ensuring continuity and efficiency in managing compliance issues. The approval or denial of extension requests will be communicated to the requester within 30 days.

VI. Remediation Capabilities and Support

When applicable, entities are encouraged to leverage OIS's statewide Security Advisory Services Program and California Department of Technology's (CDT) Critical Services and Modernization Team to ensure prompt and efficient implementation of mitigating controls to manage identified risks effectively. Cabinet-level Agency Directors (or their equivalents/delegates) are encouraged to develop strategies to mitigate risks and ensure compliance for the organizations within their agency. Directors of state entities (or their equivalents/delegates) must collaborate with their Cabinet-level Agency Directors (or their equivalents/delegates) in reporting non-compliance.

Authoritative Sources

Per GOV 11549.3, the Office of Information Security is responsible for ensuring compliance with information security and privacy policies and standards. Relevant legislative references and guidelines include, but are not limited to:

GOV	11545 – 11548 Department of Technology 11549 - 11549.4 Office of Information Security 11549.5 - 11549.10 Office of Privacy Protection
SAM	4800 Department of Technology 4819.34 Project Approval Authority 4900 Information Technology 4903.2 Information Management Costs 4983.1 Cloud Computing Policy 4989 Desktop and Mobile Computing Policy 4989.2 Definition of Desktop and Mobile Computing 4989.8 Policy Compliance 5300 Office of Information Security 5305 Information Security Program 5305.1 Information Security Program Management 5305.6 Risk Management

	5305.7 Risk Assessment 5330 Information Security Compliance 5330.2 Compliance Reporting
SIMM	18 IT Exemptions 55 Information Technology Cost Report 160 Maintenance and Operations Plan Guidelines 5300 Information Security
Technology Letters	23-03 Cloud Computing Policy 17-01 IT Cost Reporting 17-02 Mobile Phone Purchasing Delegation

Questions

Questions regarding this standard may be sent to:

California Department of Technology
Office of Information Security
Security@state.ca.gov