CalSAWS Job Description

INFORMATION SECURITY OFFICER

Salary Determined by Employer
RGS Salary Range:
$10,410.21- $16,527.78 Monthly

JOB DESCRIPTION

Under the general direction of the Chief Information Security Officer (CISO), the Information Security Officer (ISO) is responsible for operationalizing and managing the CalSAWS Information Security Program. The ISO translates enterprise security strategy (as defined by the CISO) into actionable controls, processes, documentation, oversight routines, and measurable program outcomes.

The ISO leads security governance, operational risk management processes, audit coordination, program compliance, security architectural system reviews, incident response coordination, and continuous improvement efforts. The ISO provides oversight of vulnerability management, vendor security compliance, SSP maintenance, and security policy implementation.

The ISO partners closely with the Security & Operations Manager to ensure security controls are implemented and operating effectively and collaborates with the Privacy Officer (or equivalent) to integrate privacy requirements into security processes, architecture reviews, incident workflows, and vendor risk assessments.

This position requires strong technical skills, leadership and people management skills, cross-functional coordination, effective communication across technical and non-technical partners, and a deep understanding of security and privacy considerations within large-scale public-sector systems.

RESPONSIBILITIES

- Governance, Risk, and Compliance (GRC)
  - Implement and manage the operational components of the Information Security Program in alignment with frameworks, policies, and strategic direction established by the CISO.
  - Coordinate and execute the risk assessment lifecycle, including evidence collection, documentation of findings, risk rating, mitigation plans, and reporting.
  - Maintain and update information security policies, standards, and procedures per CISO direction; ensure vendor and internal team adherence through oversight and monitoring.
  - Lead the operational coordination of state, federal, and independent audits, including evidence gathering, scheduling, documentation management, and corrective action tracking.
  - Maintain System Security Plans (SSPs), control documentation, and continuous monitoring evidence; partner with the Security & Operations Manager to verify operational control implementation.
  - Perform Third-party security risk assessments; escalate strategic risks or systemic issues to the CISO with recommended actions.
  - Integrate privacy-related requirements into security processes and documentation in partnership with the Privacy Officer.

- Privacy Alignment & Data Protection Integration
  - Partner with the Privacy Officer (or equivalent) to incorporate privacy requirements into security processes, risk reviews, vendor assessments, and system change workflows.

- Ensure technical implementation of privacy-related safeguards, including access controls, logging, encryption, and secure data handling practices.
- Support privacy investigations and privacy impact assessments by providing technical evidence, system insight, and control verification.
- Ensure incident response workflows include privacy considerations, including escalation and reporting requirements.
- Serve jointly with the Privacy Officer (or equivalent) as a resource to counties, DHCS, CDSS, CWDA, and vendors on integrated security and privacy practices.

- Security Program Implementation & Oversight
  - Translate CISO-directed strategy into program plans, maturity roadmaps, and measurable program deliverables.
  - Develop and maintain enterprise security KPIs and dashboards for leadership, governance bodies, and vendor oversight.
  - Oversee the vulnerability management program and collaborate with the Security & Operations Manager to support timely remediation.
  - Review technical and architectural designs, architecture changes, system enhancements, and vendor proposals for adherence to established policies and security/privacy requirements.
  - Identify program-level gaps and control deficiencies; recommend solutions and monitor corrective actions to completion.
  - Ensure program documentation and controls remain consistent with state and federal expectations for systems handling sensitive data.

- Incident Response Coordination
  - Serve as operational coordinator for medium-severity security incidents, ensuring proper documentation, containment oversight, and after-action reviews.
  - Collaborate with the Security & Operations Manager and vendors to ensure incidents are managed in alignment with defined procedures and SLAs.
  - Escalate major incidents to the CISO and support communications to leadership and oversight partners.
  - Conduct incident response exercises and readiness assessments to strengthen preparedness across CalSAWS and county partners.
  - Partner with the Privacy Officer (or equivalent) to assess privacy implications of security incidents and support breach-related workflows.

- Stakeholder Engagement & Cross-Functional Collaboration
  - Serve as an advisor across internal teams, counties, vendors, and state partners on security and privacy integration.
  - Provide oversight and guidance to the Security & Operations Manager to ensure consistent implementation of required controls.
  - Represent Information Security in governance meetings, vendor reviews, and cross-functional workgroups.
  - Communicate program posture, risks, and findings to leadership in a clear and accessible manner.
  - Ensure consistent application of security and privacy controls across CalSAWS' multi-vendor, multi-county environment.

DESIRABLE SKILLS AND CAPABILITIES

Candidates of this position should have applicable experience, skills, and capabilities to perform the following functions and activities:

Demonstrated experience with:

- Security frameworks, security governance practices, and compliance frameworks including NIST 800-53, SOC 2 Type 2, among others
- Cloud infrastructure such as AWS
- State and federal privacy expectations relevant to human services programs.
- Security Governance, Risk, and Compliance
- Risk assessment methodologies, documentation practices, and audit processes.
- Third party risk assessment methodology
- Security architectural reviews
- Security architecture concepts, IAM principles, encryption, logging, and monitoring.
- Vendor management and multi-vendor coordination practices.

Ability to:

- Operationalize security strategy into well-managed programs and processes.
- Mature security programs
- Lead cross-functional efforts involving technical and non-technical stakeholders.
- Analyze complex issues and provide action-oriented recommendations.
- Communicate effectively to executive leadership, counties, vendors, and oversight bodies.
- Manage multiple priorities in a complex, fast-paced environment.
- Exercise discretion and maintain confidentiality.

Working Relationships:

- The ISO works closely with:
- Chief Information Security Officer (CISO)
- Security & Operations Manager
- Privacy Officer
- Infrastructure, PMO, and Quality Assurance teams
- Vendor partners
- State & county partners
- Audit and oversight organizations

QUALIFICATIONS AND REQUIREMENTS:

MINIMUM QUALIFICATIONS

TRAINING AND EXPERIENCE:

Bachelor's degree in Information Security, Computer Science, Information Systems, or a related field. Master's degree preferred.

Five (5) years of progressive experience in information security, including risk management, compliance, or security program administration.

Two (2) years of program leadership, governance, or supervisory experience.

Experience supporting audits, maintaining security documentation, or verifying control effectiveness preferred.

Experience working in large-scale enterprise or public-sector environments is strongly preferred.

Certifications (Preferred)

- CISSP, CISM, CRISC, CCSP, or equivalent security certifications.
- Privacy certifications (CIPP/US, CIPT) are desirable.

- ITIL or similar operational framework certifications a plus.

IDENTIFICATION:

A valid California Class C Driver License or the ability to utilize an alternative method of transportation when needed to carry out job-related essential functions.

PHYSICAL CLASS:
2 - Light.

OTHER REQUIREMENTS:
ISO is expected to live within a commutable distance from Sacramento, CA.

SPECIALTY REQUIREMENTS:
N/A