

DUTY STATEMENT

DS 3022 (10/2025)

**DEPARTMENT OF DEVELOPMENTAL SERVICES
INFORMATION TECHNOLOGY DIVISION
INFORMATION SECURITY BRANCH
RISK AND COMPLIANCE UNIT**

DUTY STATEMENT

JOB TITLE: Information Technology Specialist I **POSITION #:** 472-508-1401-XXX

WORKING TITLE: Risk and Compliance Specialist

EMPLOYEE:

POSITION DESCRIPTION: Under direction of the Information Technology Supervisor II, in the Risk and Compliance Unit, the Information Technology Specialist I (ITS I) position is responsible for supporting both security and privacy within the Information Security Branch (ISB) in their mission to ensure the Department remains in compliance with state and federal requirements. The incumbent provides coordination and support in preparing, reviewing, and updating compliance materials. The incumbent also supports section staff with the submission and routing of required documents and reports to remain in compliance.

DOMAINS: Business Technology Management:	Moderate skills
Client Services:	Moderate skills
Information Security Engineering:	Basic skills
IT Project Management	Moderate skills
Software Engineering	Basic skills
Systems Engineering	Basic skills

SUPERVISION EXERCISED: None.

SUPERVISION RECEIVED: Under direction of the Information Technology Supervisor II in the Risk and Compliance Unit.

EXAMPLES OF DUTIES:

Essential Job Functions:

30% Assess the maturity of security controls using Cal-Secure, National Institute of Standards and Technology (NIST) CSF 2.0, Health Insurance Portability and Accountability Act (HIPAA) Security Rule requirements, and Zero Trust Architecture principles. Develop customized scorecards for the Department and each regional center focused on asset management, access control, and protective technologies.

Conduct community interviews to verify information, validate documentation, and ensure accuracy of assessment results.

- 20% Audit regional center adherence to HIPAA Security Rule provisions applicable to Covered Entities and Business Associates. Review whether local policies and procedures exist and are maintained, using provided templates for benchmarking. Document findings and track remediation progress.
- 20% Prepare and support audits and ensure that the Department meets audit requirements across systems and applications in scope. Assist in developing and delivering Security and Privacy training for the Department's internal program and present Security and Awareness training to all 21 regional centers.
- 10% Generate detailed gap analysis documents with mappings to NIST CSF subcategories. Recommend control improvements and evaluate implementation feasibility per site. Provide actionable recommendations with risk prioritization.
- 10% Work with IT teams to integrate survey results into a centralized system. Build automation scripts for asset discovery and compliance tracking. Collaborate on dashboards that visualize security control coverage.
- 5% Coordinate with regional center IT managers, external vendors, and internal compliance teams. Lead site debriefings and consolidate findings into cross-site comparative matrices

Marginal Job Functions:

- 5% Other duties as assigned within the scope of the classification.

WORKING CONDITIONS: Open-space partitioned offices. Occasional travel may be required. This position is a hybrid, in-office/telework position, and may be subject to change. Incumbent can be required to report to the office, or any designated location at any time. Telework agreements can be modified and/or cancelled at any time.

DESIRABLE QUALIFICATIONS:

Knowledge of: Federal and State privacy and security standards such as HIPAA and NIST; Zero Trust Architecture principles; excellent communications skills; preparing written process and procedures documents for the Information Technology Division; coordination skills, decision-making, attention to detail, and problem-solving skills.

Ability to: Research, prepare and plan organizational initiatives; manage multiple tasks, work well under deadlines, and embrace a team-oriented philosophy and environment; participate and/or present in workgroups, leadership briefings; draft, revise and/or edit documents, policies, memos, notices, or reports; develop and maintain cooperative and harmonious relationships with Department staff and colleagues; analyze situations

accurately and take effective action; communicate effectively; reason logically and creatively; and analyze data and present ideas and information effectively; contribute to the professional standing of the Department through continued education and the pursuit of professional audit certification, such as Certified Internal Auditor (CIA) and Certified Information Systems Auditor (CISA), Certified in Risk and Information Systems Control (CRISC).

CERTIFICATION OR LICENSE: None.

Employee Name
(Print)

Employee Signature

Date

Supervisor Name
(Print)

Supervisor Signature

Date

Employee and Supervisor acknowledge that by signing this Duty Statement that they have discussed and agree to the expectations of the position.