State of California - Department of Social Services
DUTY STATEMENT

EMPLOYEE NAME:	
VACANT	
CLASSIFICATION:	POSITION NUMBER:
Information Technology Specialist I	721-1402-910
DIVISION/BRANCH/REGION: *(UNDERLINE ALL THAT APPLY)*	BUREAU/SECTION/UNIT: *(UNDERLINE ALL THAT APPLY)*
ISD/ISPO	Risk & Governance
SUPERVISOR'S NAME:	SUPERVISOR'S CLASS:
Celia Khamphanh	Info. Technology Supervisor II

SPECIAL REQUIREMENTS OF POSITION *(CHECK ALL THAT APPLY)*:

- ☐ Designated under Conflict of Interest Code.
- ☐ Duties require participation in the DMV Pull Notice Program.
- ☐ Requires repetitive movement of heavy objects.
- ☐ Performs other duties requiring high physical demand. *(Explain below)*
- ☐ None
- ☑ Other *(Explain below)*

Fingerprinting clearance required.

I certify that this duty statement represents an accurate description of the essential functions of this position.		I have read this duty statement and agree that it represents the duties I am assigned.	
SUPERVISOR'S SIGNATURE	DATE	EMPLOYEE'S SIGNATURE	DATE

SUPERVISION EXERCISED *(Check one)*:

☑ None ☐ Supervisor ☐ Lead Person ☐ Team Leader

FOR SUPERVISORY POSITIONS ONLY: Indicate the number of positions by classification that this position DIRECTLY supervises.

Total number of positions for which this position is responsible:

FOR LEADPERSONS OR TEAM LEADERS ONLY: Indicate the number of positions by classification that this position LEADS.

MISSION OF ORGANIZATIONAL UNIT:

The Information Systems Division's (ISD) mission is to develop, support, and promote the business value of IT through reliable, cost-effective business processes.

The Information Security & Privacy Office mission is to provide management and oversight of the CDSS Information Security and Privacy Program ensuring protection of CDSS information assets and compliance with state and federal policies and laws.

CONCEPT OF POSITION:

Under the direction of the Information Technology Supervisor II (IT Sup II), Risk & Governance Unit. The ITS1 supports the department's information security and compliance programs by coordinating audit activities, validating security controls, maintaining risk and governance documentation, and analyzing the impact of cybersecurity and regulatory requirements. The ITS1 provides technical consultation, develops compliance reports and guidance materials, and helps ensure ongoing readiness with standards such as NIST, SAM, SIMM, HIPAA, SSA TSSR, and IRS 1075.

A. RESPONSIBILITIES OF POSITION:

40% Audit, Assessment, and Security Control Validation:
• Facilitate the collection, validation, and organization of technical, operational, and security control documentation required for external audits, reviews, and assessments, including OIS, IRS, HIPAA, CMS, and other applicable state or federal oversight activities.
• Perform detailed technical reviews of audit evidence, system documentation, security control artifacts, policies, procedures, configuration records, and related materials to assess accuracy, completeness, consistency, and alignment with applicable control requirements (NIST 800-53, SIMM 5300-A, SSA TSSR, IRS Pub 1075).
• Coordinate audit preparation activities by scheduling and documenting technical discussions, tracking evidence requests, identifying documentation gaps, and working with program, security, privacy, infrastructure, and system teams to support timely audit response.
• Serve as a technical liaison during audit and assessment engagements by providing clarification on system configurations, control implementation, operational processes, remediation activities, and supporting documentation.

30% Risk and Compliance Documentation:
• Analyze, maintain, and validate information security risk registers, compliance repositories, Plan of Action and Milestones records, control documentation, and related governance, risk, and compliance artifacts.
• Review audit findings, assessment results, control gaps, and corrective action items to support the development of remediation plans, risk treatment recommendations, and compliance strategies.
• Monitor and report on timelines for audit deliverables, corrective actions, remediation milestones, recurring compliance obligations, and evidence submissions; identify risks, delays, dependencies, and issues requiring management attention.
• Recommend, develop, and refine documentation standards, templates, procedures, and tracking methods to improve consistency, audit readiness, evidence quality, and compliance reporting practices.

20% Cybersecurity Research, Impact Analysis, and Compliance Reporting:
• Conduct independent research on emerging cybersecurity regulations, audit frameworks, state and federal requirements, security standards, privacy requirements, and industry best practices relevant to departmental systems, including changes to NIST SP 800-series publications, State Administrative Manual (SAM 5300), SIMM updates.
• Evaluate changes in laws, regulations, standards, policies, frameworks, and oversight requirements; prepare impact analyses identifying potential effects on internal systems, technical controls, operational processes, documentation requirements, and compliance obligations.
• Draft and update technical reports, dashboards, risk summaries, audit briefings, compliance status reports, and decision-support materials to communicate findings, risks, trends, remediation progress, and recommendations to technical and non-technical stakeholders.
• Develop guidance materials, process documentation, knowledge resources, and internal reference materials to support consistent implementation of audit, risk, compliance, and security documentation practices.

10% Technical Consultation, Process Improvement, and General Support:
• Participate in technical working sessions, trainings, control reviews, security initiatives, and cross-functional discussions to support audit readiness, risk management, compliance monitoring, and information security program objectives.
• Provide technical and analytical consultation to senior staff and stakeholders on projects involving cybersecurity compliance, system documentation, control implementation, audit readiness, remediation tracking, and process improvement.
• Identify and recommend improvements to compliance workflows, evidence collection methods, documentation practices, reporting processes, and audit preparation activities.
• Perform related duties in support of enterprise information security, risk management, audit readiness, privacy, and compliance functions.

B. SUPERVISION RECEIVED:

ITS1 is under the direction of the IT Supervisor II.

C. ADMINISTRATIVE RESPONSIBILITY:

None

D. PERSONAL CONTACTS:

ITS1 may have contact with CDSS executives, program management, rank and file staff, other State departments and various vendors and consultants. The ITS1 is required to maintain a professional working relationship with all customers.

E. ACTIONS AND CONSEQUENCES:

The ITS1 must ensure that CDSS is in compliance with applicable information security policies. Failure to enforce these policies can result in CDSS paying penalties and other costs.

F. OTHER INFORMATION:

Requires operating a computer terminal approximately 80% of the time, in addition to remote work. Subject to fingerprinting and criminal record clearance by the Department of Justice (DOJ) and Federal Bureau of Investigation (FBI). Travel may be required. Will attend meetings in person and remotely.

- CISSP, ISACA CISM, CompTIA Security + and (ISC)2 SSCP are desirable certifications.
- Knowledge of HIPAA, SAM 5300, NIST 800-53, NIST CSF, IRS Pub 1075
- A demonstrated interest in assuming increasing responsibility.
- Mature judgment, poise, tact, and discretions.
- Ability to take and follow directions from supervisors.
- Ability to effectively demonstrate exceptional writing and communication skill