California Department of Tax and Fee Administration

DUTY STATEMENT

☐ CURRENT
☐ PROPOSED

SCHEDULE TO BE WORKED/WORKING HOURS		EFFECTIVE DATE	
CIVIL SERVICE CLASSIFICATION	**PRIMARY DOMAIN**	**WORKING TITLE**	
Information Technology Specialist II	Information Security	Security Governance & Assurance (SGA) Lead	
DIVISION/OFFICE/UNIT		**SPECIFIC LOCATION ASSIGNED TO**	
TSD/ISO/Security & Governance Assurance Unit			
SEERA DESIGNATION	**BARGAINING UNIT**	**WORK WEEK GROUP**	**CERTIFICATES REQUIRED**
Rank and File	01	E	None
FINGERPRINTS/ BACKGROUND CHECK REQUIRED	**BILINGUAL POSITION**	**SUPERVISION EXERCISED**	
☒ Yes ☐ No	☐ Yes ☒ No	Act as lead	
INCUMBENT		**POSITION NUMBER** *(Agency-Unit-Class-Serial)*	
		291 - 381 - 1414 -	

The mission of the California Department of Tax and Fee Administration is to make life better for Californians by fairly and efficiently collecting the revenue that supports our essential public services.

POSITION'S ORGANIZATIONAL SETTING AND MAJOR FUNCTIONS

Under direction of the Deputy Chief Information Security & Privacy officer (IT Manager I), the Information Technology Specialist II (IT Spec II) serves as the lead of the Security Governance and Assurance Team (SGA) in the Information Security Office (ISO). The IT Specialist II leads efforts to establish and maintain a consistent and efficient risk management program, privacy program and a vulnerability management program while ensuring alignment and compliance with statewide and federal requirements and integration of risk-based decision-making across IT and business units.

Candidate must be able to perform the following essential job functions with or without reasonable accommodation.

PERCENTAGE OF TIME SPENT	DUTIES
	ESSENTIAL JOB FUNCTIONS
25%	**Security Governance and Assurance Lead** The Security Governance and Assurance Lead provides expert operational leadership for information security governance and assurance activities within the Information Security Office. Ensures compliance with NIST Special Publications (SP) 800 53, IRS Publication 1075, the State Administrative Manual (SAM), and the Statewide Information Management Manual (SIMM) while maintaining alignment with recognized industry best practices. The Lead serves as the Subject Matter Expert (SME) for the most complex information security governance policies, procedures, standards, processes, requests, and projects. The position oversees security governance work activities to ensure timely and accurate resolution of requests and issues. The position oversees, conducts and provides guidance to Security Governance and Assurance team members regarding security related assessments, audits, compliance monitoring and enforcement, and other information security governance duties as required. The Lead is responsible for driving continuous improvement of security governance methodologies and assurance functions, ensuring they remain effective, efficient, and aligned with organizational and regulatory requirements.
20%	**Vulnerability Management Program** • Oversee, direct, manage and lead the department's vulnerability management program. • Ensure continuous identification, assessment and remediation of security flaws. • Leverage frameworks such as Common Vulnerability Scoring System (CVSS) to assist with prioritizing patching based on the exploitability of said vulnerabilities and the criticality of the affected resource to CDTFA daily operations. • Partner with IT Infrastructure, Application Development and IT operations to enforce patch management policies and Service Level Agreements (SLAs). • Facilitate and monitor the remediation process and ensure that validation occurs to verify that the patch, configuration or compensating controls have been applied. • Ensure all delayed remediations or ones that did not meet the SLA are tracked and managed through the risk management program and ensure remediation plans are documented and approved by management or have executive sign-off if needed.

- Develop, track and distribute vulnerability metrics to Chief Information Security Officer (CISO) and Chief Information Officer (CIO).

20%

Risk Management Program

- Lead, implement, and enforce the information security risk management program.
- Lead, plan, prepare, present and perform risk assessments for CDTFA's information systems.
- Ensure continuous risk identification, evaluation and mitigation of privacy and security risks are aligned with (NIST) Special Publications (SP) 800-37 and adhere to IRS Pub 1075, SAM, SIMM requirements.
- Assists in the maintenance of the security risk register and plan of action and milestones (POAM).
- Collaborate with risk owners on remediation and mitigation of risks.
- Evaluate the effectiveness of the proposed and implemented controls and mitigations to quantify the residual risk.
- Facilitate and lead the formal risk acceptance and exception process for compliance gaps or findings that cannot be adhered to due to operational or technical constraints.
- Provide guidance to the Deputy CISO and CISO as to what is an acceptable risk.

15%

Privacy Program

- Lead, implement and conduct comprehensive Privacy Threshold Assessments (PTAs) and Privacy Impact Assessment (PIAs) on new and existing information systems and applications.
- Ensure all privacy risks are identified and tracked via the risk management program to ensure they are remediated.
- Assists with the development, creation, and management of enterprise privacy, data classification, and data loss prevention program to ensure compliance with state, federal, and other regulatory requirements, as well as ensuring the confidentiality, integrity, and availability of CDTFA's data.
- Assist and provide guidance to the data governance program and ensure best practices to privacy are applied to all systems and applications such as data minimization, mapping, inventories, flows, retention schedules, privacy by design, role-based access and privacy training.
- Serve as the Subject Matter Expert (SME) for privacy incidents involving PII, confidential tax information or FTI.
- Collaborates cross-functionality with IT staff, Disclosure Office, Legal and Business Programs to determine the scope and root cause of the privacy incidents.
- Ensure privacy incidents are reported as required by state and federal requirements.
- Oversee and assist with drafting any breach notices, post incident/lessons learned review, and enforce Corrective Action Plans (CAPs) to prevent future incidents.

10%

Information Security Policy and Consultation

- Provide technical security guidance, consultation in security policy, security design, system hardening, software development, risk management and compliance.
- Make appropriate risk-based recommendations with the purpose of securing information systems.
- Collaborates cross-functionally to develop and maintain information security standards and controls to support policy compliance.
- Maintains exceptional knowledge and up-to-date perspective on evolving security trends, standards, and best practices with a focus on system security and governance.
- Formulate and maintain information security policies and ensure alignment and adherence to NIST 800-53, IRS Pub 1075, SAM, SIMM publications and industry best practices.

MARGINAL JOB FUNCTIONS

10%

Provides support and coverage for other ISO team members as needed and perform other job-related duties as required.

WORK ENVIRONMENT OR PHYSICAL ABILITIES REQUIRED FOR THE JOB (if applicable):

Work Environment:

- May work in a high-rise building
- Standard office environment (for example, artificial lighting, controlled temperature, etc.)
- Requires being in a stationary position, consistent with office work, for extended periods of time
- Daily use of a personal computer, office equipment, and/or telephone

Physical Abilities:

-

Additional Requirements/Expectations:

-

I have read this duty statement and fully understand that I must perform the Essential Job Functions of my position with or without reasonable accommodation.

PRINT EMPLOYEE NAME	EMPLOYEE'S SIGNATURE	DATE

I certify that the above accurately represents the duties of the position and that I have reviewed these duties with the above-named employee.

PRINT SUPERVISOR NAME	SUPERVISOR'S SIGNATURE	DATE

HRB Approval Date: 09/10/2026	C&P Analyst Initials: LLM