Employment Development Department
State of California

☐ Current
☒ Proposed

POSITION STATEMENT

1. POSITION INFORMATION

CIVIL SERVICE CLASSIFICATION:	WORKING TITLE:
Information Technology Specialist II	Senior Risk Assessment Analyst
NAME OF INCUMBENT:	POSITION NUMBER:
Click here to enter text.	280-390-1414-976
OFFICE/SECTION/UNIT:	SUPERVISOR'S NAME:
Privacy & Integrated Risk Management Office/Integrated Risk Management Group	Christopher Kashuba
DIVISION:	SUPERVISOR'S CLASSIFICATION:
Cyber Security Division	Information Technology Manager I
BRANCH:	REVISION DATE:
Information Technology Branch	8/8/2023

Duties Based on: ☒ FT ☐ PT– Fraction _____ ☐ INT ☐ Temporary – _____ hours

2. REQUIREMENTS OF POSITION

Check all that apply:

☒ Conflict of Interest Filing (Form 700) Required
☐ May be Required to Work in Multiple Locations
☐ Requires DMV Pull Notice
☐ Travel May be Required
☐ Call Center/Counter Environment
☒ Requires Fingerprinting & Background Check
☐ Bilingual Fluency *(specify below in Description)*
☐ Other *(specify below in Description)*

Description of Position Requirements:
(e.g., qualified Veteran, Class C driver's license, bilingual, frequent travel, graveyard/swing shift, etc.)

3. DUTIES AND RESPONSIBILITIES OF POSITION

Summary Statement:
(Briefly describe the position's organizational setting and major functions)

Information Technology Domains (Select all domains applicable to the incumbent's duties/tasks.)

☐ Business Technology Management ☒ IT Project Management ☐ Client Services
☒ Information Security Engineering ☐ Software Engineering ☐ System Engineering

Under general direction of the Information Technology Manager I (ITM I), the Information Technology Specialist II, serves as the technical lead driving ongoing development and maintenance of EDDs risk assessment processes performing targeted risk assessments, pen testing, produces quality professional work products, including risk assessment reports. Works with system owners to plan, schedules risk assessment schedules, tests, develop, updates and maintains system security plans, Risk Register Plan of Action and Milestone, system and process security risk assessments and prepares certification and accreditation packages.

Civil Service Classification **Position Number**

Information Technology Specialist II

Percentage of Duties	Essential Functions
40%	The IT Spec II's responsibilities include cyber defense monitoring, tracking, and processing of risk Acts as a lead in the performance of information security risk management activities including: • Perform technical risk and vulnerability assessments of relevant technology focus areas (e.g., local computing environment, network and infrastructure, enclave boundary, supporting infrastructure, and applications). • Make recommendations regarding the selection of cost-effective security controls to mitigate risk. • Prepares system security plans, certification and accreditation packages, and security consulting services to assist lines of business in identifying and mitigating vulnerabilities within their respective information technology environments. • Monitors, tracks and reports security risks and vulnerabilities, identifies steps to remediate security gaps, reporting and maintaining risk registers and tracks the successful completion of remediation activities. • Leads authorized penetration testing in a manner that is compliant with the department's requirements and the rules of engagement. • Advises and consults EDD's lines of business to ensure they are developing, operating, and maintaining secure systems.
40%	Performs security evaluations and audits of software/systems/applications/processes including: • Tracking risk findings in risk assessment reports and logs in Risk Register Plan of Action and Milestones (RPOAM), driving RRPOAM items to closure, and reporting progress to internal stakeholder to help EDD programs to maintain information security (IS) compliance and avoid or minimize adverse impact to EDD stakeholders. • Collaborates with management in developing and implementing risk management operational security policies and procedures that satisfy federal and state regulations. • Leads efficient IT risk management operations that enable business programs to achieve their goals without exposure to compliance issues. • Analyzes security gaps identified by risk management practices and documents recommended actions. Coordinates and leads meetings to drive resolution of technical, federal, State, and internal audit findings. Conducts ongoing assessments of the most complex processes and systems, analyzes impacts and risk exposure, and develops recommended solutions to minimize security threats and vulnerabilities. • Implements cybersecurity reporting and procedures and collaborates with the Enterprise Security Operations Section (ESOS) Security Architect, and other Infrastructure Services Division (ISD)/ESOS teams in the planning, coordination, and direction of a wide variety of security risk and compliance-related work. • Conduct required reviews as appropriate within environment.
15%	The IT Spec II provides technical advice and consultation on all phases of the project management and secure system development life cycles to ensure efficient, effective, and secure delivery of unique IT product, service, or system. The IT Spec II will assist in describing the scope of work, objectives, tasks, and resources needed to successfully plan the IT projects for the organization's mission. As part of the IT portfolio, the candidate must collaborate with its business partners, prioritize IT projects, collaborate in selecting high value opportunities to enhance services, and effectively and efficiently operate the organization's IT resources. • Develops and manages the work breakdown structure (WBS) of IT projects. • Develops or updates project plans for IT projects including information such as project objectives, technologies, security, systems, information specifications, schedules, funding, and staffing.

	• Leads project teams, which may include business analysts, system engineers, security analysts, system architects, subject matter experts, test coordinators, external entities, and users on the State and departmental project management methodologies to ensure project compliance with State policies. • Integrates information systems and/or subsystems as designed. • Manages project(s) to ensure adherence to budget, schedule, and scope. • Determines the resources (time, money, equipment, staffing, etc.) required to complete the project. • Develops implementation plans that take into consideration analyses such as cost-benefit or return on investment. • Directs the conduct of integrated change control processes. • Makes changes to identification of infrastructure configuration, security, and change management standards or requirements. • Manages or oversees one or more IT security projects applying industry standards, principles, guidelines, methods, techniques, security, using planning, monitoring, processes, and controlling principles tools to deliver an IT product, program solution, service, or system. • Prepares documentation using standard California Project Management Frameworks or Methodologies. The IT Spec II provides input for the incident response teams relating to the security aspects of the initiation, design, development, testing, operation, security, and defense of IT environments to address sources of disruption, ranging from natural disasters to malicious acts. Responsibilities include but are not limited to: • Supports EDD's information security incident response and reporting activities. Actively responds to security incidents using playbook and security techniques accordingly. • Collaborates with impacted stakeholders to ensure accurate and timely incident resolution by properly following procedures throughout the incident handling process of identification/investigation, containment, eradication, recovery, and lessons learned. • Coordinates in the testing, implementation, deployment, reviews, and administration of infrastructure hardware and software that are required to effectively manage the EDD computer network, service provider network and resources. • Analyzes business impact and exposure, based on emerging security threats, vulnerabilities, and risks and provided recommend IT solutions. • Categorizes the information system and the information processed, stored, and transmitted by that system. • Develops and ensures security solutions and technical artifacts are in place throughout all IT systems and platforms. • Monitors and assesses security controls in the information system on an ongoing basis, documenting changes, conducting security impact analyses, and reporting system security statuses to the organization.
Percentage of Duties	**Marginal Functions**
5%	Performs other duties as assigned.

4. WORK ENVIRONMENT *(Choose all that apply)*

Standing: Occasionally - activity occurs < 33%	Sitting: Continuously - activity occurs > 66%
Walking: Occasionally - activity occurs < 33%	Temperature: Temperature Controlled Office Environment
Lighting: Artificial Lighting	Pushing/Pulling: Not Applicable - activity does not exist
Lifting: Not Applicable - activity does not exist	Bending/Stooping: Not Applicable - activity does not exist
Other: *Click here to enter text.*	

Civil Service Classification
Information Technology Specialist II

Position Number

Type of Environment:
☐ High Rise ☒ Cubicle ☐ Warehouse ☐ Outdoors ☐ Other**:**

Interaction with Customers:
☐ Required to work in the lobby
☐ Required to work at a public counter
☐ Required to assist customers on the phone
☐ Required to assist customers in person
☐ Other:

5. SUPERVISION EXERCISED:
(List total per each classification of staff)

Provides lead person directions to lower-level Information Technology Specialist staff on Integrated Risk Management (IRM) team.

6. SIGNATURES

Employee's Statement:
I have reviewed and discussed the duties and responsibilities of this position with my supervisor and have received a copy of the Position Statement.

Employee's Name:

Employee's Signature: Date:

Supervisor's Statement:
I have reviewed the duties and responsibilities of this position and have provided a copy of the Position Statement to the employee.

Supervisor's Name:

Supervisor's Signature: Date:

7. HRSD USE ONLY

Personnel Management Group (PMG) Approval

☒ Duties meet class specification and allocation guidelines. ☐ Exceptional allocation, STD-625 on file.	PMG Analyst Initials	Date Approved
	dmg	8/8/2023

Reasonable Accommodation Unit use ONLY *(completed after appointment, if needed)*
If a Reasonable Accommodation is necessary, please complete a Request for Reasonable Accommodation (DE 8421) form and submit to Human Resource Services Division (HRSD), Reasonable Accommodation Coordinator.

List any Reasonable Accommodations made:

Supervisor: After signatures are obtained, make 2 copies:

- Send a copy to HRSD (via your Attendance Clerk) to file in the employee's Official Personnel File (OPF)
- Provide a copy to the employee
- File original in the supervisor's drop file