CALIFORNIA High-Speed Rail Authority

Job Description

Position Details

Classification:
Information Technology Specialist II

Office:
Information Technology

Working Title:
Information Security Specialist

Location:
Sacramento

Position Number:
311-420-1414-004

HR Approval Date/Initials:
05/21/26 FAY

CBID/Bargaining Unit:	Work Week Group:	Tenure:	Time Base:
R01	E	Permanent	Full-Time

Job Description Summary

Under the general direction of the Security Operations Manager, an Information Technology (IT) Manager I of the California High-Speed Rail Authority (Authority), the IT Specialist II (Information Security Specialist) serves as a lead for the Enterprise Governance, Risk, and Compliance (GRC) section. The incumbent works independently and collaboratively to plan, implement, maintain, and oversee the Authority's enterprise-wide GRC activities, with a strong focus on identifying, assessing, and managing information security risks. As a technical specialist within the Authority's Information Security Program, the incumbent provides leadership in the development, documentation, and maintenance of information security policies, standards, and procedures; ensures effective configuration management practices; and coordinates enterprise reporting on governance, risk posture, privacy, and compliance performance.

The incumbent leads efforts to establish and maintain a consistent, repeatable risk management framework; ensures alignment with statewide and federal requirements; and drives integration of risk-based decision-making across IT and business units. Through expert-level guidance and oversight of risk identification, evaluation, mitigation, and monitoring activities, the incumbent strengthens the Authority's security governance and elevates organizational risk awareness and accountability. These efforts enhance the Authority's ability to manage enterprise security risk effectively and support the protection of critical assets in alignment with mission objectives.

The following IT Domains are applicable to the incumbent's duties/tasks:

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

Duties
Percentage
Essential (E)/Marginal (M)

35% (E) **Risk Management**

- Leads the development and maintenance of the Authority's information security risk management framework.
- Conducts risk assessments for systems, projects, changes, and third-party services using standardized methodologies.
- Maintains the enterprise risk register and ensures risks are accurately scored, categorized, and prioritized.
- Coordinates with system owners to validate risk impacts and define appropriate mitigation strategies.
- Tracks and reports the status of risk treatment plans, ensuring timely mitigation, acceptance, or escalation.
- Provides risk-based recommendations during architecture reviews, procurements, and system design discussions.
- Monitors emerging threats, technology changes, and business processes to identify new or evolving risks.
- Produces risk dashboards, summaries, and metrics for leadership and governance bodies.
- Ensures alignment between risk assessments, Plans of Action and Milestones (POAMs), audit findings, and security exception requests.
- Serves as a primary resource for auditors and stakeholders requiring risk documentation or clarification.

20% (E) **Policies, Standards, and Procedures Development**

- Drafts, reviews, and maintains security policies, technical standards, and operating procedures in alignment with State Administrative Manual (SAM), Statewide Information Management Manual (SIMM), National Institute of Standards and Technology (NIST), and industry best practices.
- Translates regulatory and statewide policy requirements into technical control requirements for IT systems and services.
- Maintains and version-controls policy and procedure documentation in centralized repositories.
- Collaborates with system administrators, developers, network engineers, and business stakeholders to validate that the documented standards are practical and enforceable.
- Develops and maintains a formal security exception register with documented risk assessments and mitigation plans.
- Creates and maintains hardening guides aligned to Center for Internet Security (CIS) Benchmarks, Defense Information

Systems Agency (DISA), Security Technical Implementation Guides (STIGs), or equivalent standards.
- Maps technical baselines to security control frameworks such as NIST SP 800-53, ISO 27001.
- Assists with drafting and maintaining System Security Plans (SSPs) and architecture diagrams for enterprise systems.
- Documents and updates data flow diagrams and architecture diagrams to reflect security controls and system boundaries.

15% (E) **Privacy Program Management and Data Loss Prevention**
- Assists with the development, creation, and management of the 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 Authority's data.
- Assesses, develops, implements, and maintains an enterprise security and privacy awareness training program, ensuring consistency with the organization's risk management strategy and priorities.
- Performs Federal Information Processing Standards (FIPS) 199, information system categorization, and data classification to assess the potential impact on Authority assets and operations should the information or information system become compromised through unauthorized access, use, disclosure, disruption, modification, or destruction.
- Monitors and reviews proposed modifications to existing systems to ensure appropriate information security and privacy safeguards are maintained.
- Develops and reviews data sharing agreements prior to release of confidential information.
- Provides technical assistance and consultation to Authority personnel regarding information security and privacy.

15% (E) **Audit, Compliance, and Reporting Support**
- Collects and organizes system-level evidence (logs, configurations, vulnerability scans, patching records) for audits, assessments, and reviews in accordance with retention requirements.
- Tracks POAMs, monitors progress, and updates remediation status.
- Supports compliance reporting by preparing metrics dashboards and control assessment summaries for management review, to demonstrate compliance with statewide information security policies.
- Maintains documentation that demonstrates continuous monitoring of security controls across Authority's systems.

- Supports collection and retention of log data, audit rails, and forensic records in accordance with retention requirements.
- Generates technical compliance metrics (e.g., patch levels, scan findings, control effectiveness) to support management reporting.

10% (E) **Communication and Awareness**

- Drafts technical bulletins and configuration guides to communicate security standards to system administrators and developers.
- Develops step-by-step technical procedures for incident response, access management, or patching workflows.
- Provides technical documentation and guidance in security governance meetings, design reviews, and project planning sessions.
- Assists in building information security knowledge base articles and maintaining internal technical guides.
- Creates technical reference sheets for IT staff covering patch management, account lifecycle, and secure coding practices.
- Documents after-action reports from security incidents, tabletop exercises, or audits and shares lessons learned with IT staff.

5% (M) **Other Duties**

- Fosters an environment of teamwork and collaboration, communicates position-related information, and promotes the exchange of ideas through active listening and open discussion.
- Actively participates in team and departmental meetings, training, technology initiatives, or other assignments in person and remotely.
- Maintains up-to-date knowledge about state policies, processes, and industry best practices related to IT administration and information security.
- Invests in personal development through continuous education to gain and enhance position-related knowledge.
-
- Ensures travel is approved and documentation and expense claims are processed in a timely manner.

Special Requirements

The checked boxes below indicate any additional requirements of this position.

License Required	Conflict of Interest (COI)	Bilingual Required	Contract Manager	Medical Required
Yes ☐ No ☒ Type:	Yes ☒ No ☐	Yes ☐ No ☒ Language:	Yes ☐ No ☒	Yes ☐ No ☒

Other Special Requirements Information:

Conflict of Interest (COI) – This position is designated under the Conflict-of-Interest Code. The position is responsible for making, or participating in the making, of governmental decisions that may potentially have a material effect on personal financial interests. The employee is required to complete Form 700 within 30 days of assuming employment. Failure to comply with the Conflict-of-Interest Code requirements may result in disciplinary action.

Knowledge and Abilities

All knowledge and abilities of the Information Technology Specialist I classification; and

Knowledge of: Emerging technologies and their applications to business processes; business or systems process analysis, design, testing, and implementation techniques; techniques for assessing skills and education needs to support training, planning and development; business continuity and technology recovery principles and processes; principles and practices related to the design and implementation of information technology systems; information technology systems and data auditing; the department's security and risk management policies, requirements, and acceptable level of risk; application and implementation of information systems to meet organizational requirements; project management lifecycle including the State of California project management standards, methodologies, tools, and processes; software quality assurance and quality control principles, methods, tools, and techniques; research and information technology best practice methods and processes to identify current and emerging trends in technology and risk management processes; and state and federal privacy laws, policies, and standards.

Ability to: Recognize and apply technology trends and industry best practices; assess training needs related to the application of technology; interpret audit findings and results; implement information assurance principles and organizational requirements to protect confidentiality, integrity, availability, authenticity, and non-repudiation of information and data; apply principles and methods for planning or managing the implementation, update, or integration of information systems components; apply the principles, methods, techniques, and tools for developing scheduling, coordinating, and managing projects and resources, including integration, scope, time, cost, quality,

human resources, communications, and risk and procurement management; monitor and evaluate the effectiveness of the applied change management activities; keep informed on technology trends and industry best practices and recommend appropriate solutions; foster a team environment through leadership and conflict management; effectively negotiate with project stakeholders, suppliers, or sponsors to achieve project objectives; and analyze the effectiveness of the backup and recovery of data, programs, and services.

Desirable Qualifications

- Associate or bachelor's degree in an IT-related field of study.
- 5 years of related experience in information security or an equivalent combination of education and experience.
- Possession of one or more of the following active certifications is desirable:
  - CompTIA Security+
  - CompTIA Cybersecurity Analyst+ (CySA+)
  - Certified Cloud Security Professional (CCSP)
  - Certified Information Security Auditor (CISA)
  - Certified Information Systems Security Professional (CISSP)
  - GIAC Continuous Monitoring Certification (GMON)
  - Microsoft Security Operations Analyst
  - AWS/Azure Security Engineer Associate
- Strong technical writing skills with the ability to produce security baselines, configuration guides, system documentation, and reports.
- Experience with system hardening and compliance frameworks such as CIS Benchmarks, DISA, STIGs, and NIST SP 800-53/171.
- Familiarity with enterprise IT environments including Windows Server, Linux, Active Directory, databases, and cloud platforms (Azure, AWS, M365).
- Hands-on experience working with IT infrastructure including routers, witches, servers, databases, and endpoint management.
- Hands-on experience with information security tools such as Security Information and Event Management (SIEM), vulnerability scanners (e.g., Tenable, Qualys), EDR platforms, and log management solutions.
- Knowledge of security devices such as network firewalls, web application firewalls, web content filters, and intrusion prevention/detection systems.
- Knowledge of networking concepts and practices.
- Knowledge of cybersecurity frameworks, governance risk assessments and compliance in the IT field.
- Ability to analyze documents to provide feedback and inform management of appropriate information.
- Understanding of scripting or automation (e.g., PowerShell, Python, or Bash) to assist with policy enforcement and evidence gathering.
- Experience authoring security policies, procedures, and other reference materials.

- Ability to adapt quickly to new tools, platforms, and security frameworks as technology and compliance requirements evolve.
- Ability to establish and maintain cooperative working relationships with all levels of staff and management; communicate effectively with peers, other technical teams, external partners, vendors, and others.
- Ability to manage multiple-high priority initiatives in a fast-paced achievement-oriented environment and work under pressure to meet deadlines.
- Ability to maintain confidentiality of sensitive tasks, assignments, and information.
- Willingness to work excess hours to achieve business results.
- Display enthusiasm for continuous learning.

Supervision Exercised Over Others

This level does not supervise but may act as a lead. The IT Specialist II has defined responsibility and authority for decision-making related to projects or in an advisory function.

Public and Internal Contacts

The incumbent will have regular contact with various levels of staff at the Authority, consultants, vendors, contractors, and staff at other state agencies. The incumbent must handle all situations and communications tactfully and respectfully to support the Authority's mission.

Responsibility for Decisions and Consequence of Error

At the Information Technology Specialist II level, the incumbent is responsible for individual decisions and actions. As a subject matter expert, this level is responsible for actions that could have a serious detrimental effect on the operating efficiency of the undertaking or function. The consequence of error at this level may result in the loss of data, user dissatisfaction, and impacts to the organization, project, or work unit, and related support units. Consequences include operational downtime, loss of business continuity, and poor customer service and performance.

Physical and Environmental Demands

While working on-site, the incumbent works in a professional office environment, in a climate-controlled area which may fluctuate in temperature and is under artificial light. The incumbent will be required to use a computer, mouse, and keyboard, and will be required to sit for long periods of time at a computer screen. The incumbent must be able to focus for long periods of time, multi-task, adapt to changes in priorities, and complete tasks or projects with short notice. The incumbent must develop and maintain cooperative working relationships and display professionalism and respect for others in all contact opportunities.

Working Conditions and Requirements

a. Schedule: Flexible schedules may be available for this position. Specific schedules will be set between the supervisor and the employee.
b. Telework: Part-time telework may be available for this position for California residents based on the requirements of the position.
c. Travel: Occasional travel to Authority locations within California to attend meetings or training, or to support business needs may be required.
d. Other: The incumbent will be required to carry a state-issued cell phone and work outside their regular schedule, as needed, to meet business needs.

Acknowledgment and Signatures

I have read and understand the duties listed above and can perform them with/without reasonable accommodation (RA). (If you believe you may require RA, please discuss this with the supervisor indicated below who will discuss your concerns with the RA coordinator. If you are unsure whether you require reasonable accommodation, inform the supervisor indicated below who will discuss your concerns with the RA Coordinator.)

Employee Printed Name:	Signature:	Date:

I have discussed the duties with and provided a copy of this duty statement to the employee named above.

Supervisor Printed Name:	Signature:	Date: