

POSITION DUTY STATEMENT

DOT PM-0924 (REV 01/2025)

CLASSIFICATION TITLE Information Technology Manager I	OFFICE/BRANCH/SECTION IT/Security Service Division	
WORKING TITLE Governance Risk Compliance Manager (GRC Manager)	POSITION NUMBER 900-170-1405-051	REVISION DATE 04/15/2026

As a valued member of the Caltrans team, you make it possible to improve lives and communities through transportation.

GENERAL STATEMENT:

Under the general direction of the Deputy Chief Information Security Officer, an Information Technology Manager II in the Security Services Division, the Information Technology Manager I is responsible for the management and oversight of the Department of Transportation's (Caltrans) Governance, Risk, Compliance, and Forensics teams in support of ensuring protection of Caltrans information assets and compliance with State information security policies, standards and procedures per the Statewide Information Management Manual (SIMM 5305-A). As the GRC Manager at Caltrans, the incumbent manages issues affecting information security, operational recovery, security incident response, and network technologies. The GRC Manager recommends, develops and oversees the implementation of policies associated with risk management industry standards to identify and assess risk associated with Caltrans' Information Security assets.

Domains: Information Security Engineering

CORE COMPETENCIES:

As an Information Technology Manager I, the incumbent is expected to become proficient in the following competencies as described below in order to successfully perform the essential functions of the job, while adhering to and promoting the Department's Mission, Vision, Values, Strategic Imperatives and Goals. Effective development of the identified Core Competencies fosters the advancement of the following Leadership Competencies: Change Commitment, Risk Appetite, Self-Development/Growth, Conflict Management, Relationship Building, Organizational Awareness, Communication, Strategic Perspective, and Results Driven.

- Flexibility and Managing Uncertainty** : Adjusts thinking and behavior in order to adapt to changes in the job and work environment. (Safety, Prosperity - Collaboration, Innovation, Integrity, Stewardship)
- Decision Making**: Makes critical and timely decisions. Takes charge. Supports appropriate risk. Makes challenging and appropriate decisions. (Safety, Prosperity - Innovation, Integrity, Pride, Stewardship)
- Ethics and Integrity**: Demonstrated concern to be perceived as responsible, reliable, and trustworthy. Respects the confidentiality of information or concern shared by others. Honest and forthright. Conforms to accepted standards of conduct. (Equity, Employee Excellence - Integrity, Pride)
- Problem-solving and Decision-making** : Identifies problems and uses logical analysis to find information, understand causes, and evaluate and select or recommend best possible courses of action. (Safety, Prosperity - Collaboration, Innovation, Integrity)
- Relationship Building**: The ability to develop and maintain internal and external trust and professional relationships, which includes listening and understanding to build rapport. (Equity, Prosperity, Employee Excellence - Collaboration, Equity, Integrity, Pride)
- Organizational Awareness**: Contributes to the organization by understanding and aligning actions with the organization's strategic plan, including the mission, vision, goals, core functions, and values. (Safety, Prosperity, Employee Excellence - Collaboration, Equity, Integrity, Pride, Stewardship)
- Interpersonal Effectiveness** : Effectively and appropriately interacts and communicates with others to build positive, constructive, professional relationships. Tailors communication style based on the audience. Provides and is receptive to feedback. (Safety, Prosperity, Employee Excellence - Collaboration, Equity, Integrity, Pride, Stewardship)
- Planning and Results Oriented**: Organizes and executes work to meet organizational goals and objectives while meeting quality standards, following organizational processes, and demonstrating continuous commitment. (Safety, Equity, Prosperity - Collaboration, Innovation, Integrity, Pride, Stewardship)
- Managing Performance**: Responsible for employee performance, setting clear goals and expectations, tracking progress against departmental and unit goals, providing feedback, and addressing performance issues promptly. (Safety, Equity, Prosperity, Employee Excellence - Collaboration, Equity, Integrity, Pride, Stewardship)

TYPICAL DUTIES:

Percentage
Essential (E)/Marginal (M)¹ Job Description

POSITION DUTY STATEMENT

DOT PM-0924 (REV 01/2025)

40%	E	The GRC Manager will provide leadership to subordinate supervisors of the Forensics Offices, while directly overseeing and managing the department's Governance Risk Compliance teams. In addition, the GRC Manager will conduct comprehensive analysis on the most complex computer systems protecting the Department's information assets including assessments and audits on the Department's infrastructure, applications, and systems to ensure compliance with the Department's policies and standards. The incumbent will lead the development of the Department's Cyber Security Roadmap and serve, with the Deputy Chief Information Security Officer, as the Department's Information Security representative for statewide information security issues, incidents, and investigations involving external parties such as the Governor's Office, the Agency Secretary, the California Information Security Office, and law enforcement agencies. Responsibilities include leading the implementation and integration of the Department's Information Security Policy & Governance, Risk Management, Technology Recovery planning, and Cyber Incident Response Plans. The incumbent will lead the processes for reporting, logging, and coordinating response to incidents affecting the security of Department resources and lead the Department Cyber Incident Response Team. The GRC Manager collaborates with Stakeholders to develop and implement policies for the Information Security Management program. The incumbent works alongside the Deputy CISO to develop short and long term strategic direction for the Security Services Division, and establishes Division Program Level Action Plans that include the Department's goals, strategic objectives, strategies and performance measures.
30%	E	The incumbent is responsible for initiating planning, executing and controlling all security project activities following the Project Management Book of Knowledge (PMBOK) Project Management methodology. In addition, the incumbent will develop Budget Change Proposals/Concepts (BCPs), Request for Quotes (RFQs), Request for Proposals (RFPs), Feasibility Study Reports (FSRs), etc., within the Department's budget cycle. Provides operations guidance to develop procedures and guidelines in the securing of network equipment and software (i.e., servers, routers, etc.); communications (i.e., hardcopy, electronic, microfilm, etc.); and media and physical security systems related to the storage or transmittal of physical security data (i.e., the network supporting the cameras on State bridges or storage of badge information). Ensures security improvement actions are evaluated, validated, and implemented. Identifies security and risk implications of new technologies. Interprets and/or approves security requirements of new technologies. Represents the Department regarding these programs with external stakeholders (i.e., Department of Finance, California Department of Technology, California Transportation Agency, and Governor's Office of Emergency Services).
20%	E	The incumbent will serve as the Security Services Division lead and subject matter expert for Department-wide projects initiated through the IT Project Management Office (PMO) or requests received from Department program areas. The incumbent will review and recommend security controls for Feasibility Study Reports (FSRs), Request for Offers, and RFPs to ensure adherence to State of California Government Code and policies. In addition, the incumbent will lead the preparation and presentation of reports on the security, integrity, and availability of information systems to Executive and Management personnel, and information security stakeholders. Develops, implements and maintains risk analysis including assessments to identify potential vulnerabilities that could threaten the security of the Department's information assets. Ensures compliance with certification and reporting requirements for the Department to its external stakeholders.
10%	M	The incumbent will provide leadership, mentoring, performance evaluation, direction, and work assignments for staff.

POSITION DUTY STATEMENT

DOT PM-0924 (REV 01/2025)

¹ESSENTIAL FUNCTIONS are the core duties of the position that cannot be reassigned.
 MARGINAL FUNCTIONS are the minor tasks of the position that can be assigned to others.

SUPERVISION OR GUIDANCE EXERCISED OVER OTHERS

The incumbent supervises classifications including IT Supervisor II, IT Specialist II, IT Specialist I, IT Associate and Staff Services a IT Supervisor II, two teams of IT professional supervisors and staff (Security Monitoring & Response and Network Security).

KNOWLEDGE, ABILITIES, AND ANALYTICAL REQUIREMENTS

Knowledge of Information technology governance principles and guidelines to support decision making; complex and mission critical business processes and systems; principles, methods and procedures for designing, developing, optimizing, and integrating systems in accordance with best practices; system specifications design, documentation, and implementation methodologies and techniques, 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. The principles of personnel management, supervision, and training; the organization's mission, policies, principles and practices; business and management principles involved in strategic planning, resource allocation, leadership technique, coordination of people and resources; principles and practices of organization, administration, personnel (recruitment, selection, training, compensation, benefits, labor relations, negotiation, and personnel information systems), and budget management; organizational roles and responsibilities and the ability to tailor training appropriately; principles and practices of employee supervision, development, and training; a supervisor's responsibility for promoting equal opportunity in hiring and employee development and promotion; maintaining a work environment which is free of discrimination and harassment; principles of personnel management, supervision, and training, a manager's responsibility for promoting equal opportunity in hiring and employee development and promotion and maintaining a work environment which is free of discrimination and harassment; the department's Equal Employment Opportunity objectives; and a manager's role in Equal Employment Opportunity and the processes available to meet equal employment objectives.

Ability to formulate and recommend policies and procedures; perform effectively in a fast-paced environment with constantly changing priorities; establish and maintain project priorities; apply federal, state, department, and organizational policies and procedures to state information technology operations; apply systems life cycle management concepts used to plan, develop, implement, operate, and maintain information systems; positively influence others to achieve results that are in the best interests of the organization; consider the business implications of the technology to the current and future business environment; communicate change impacts and change activities through various methods; conduct end-user training; collaborate closely with technical subject matter experts such as database administrators, network engineers, and server administrators to ensure systems are secure and meet compliance requirements; assess situation to determine the importance, urgency, and risks to the project and the organization; make decisions which are timely and in the best interests of the organization; provide quality and timely ad hoc project information to executives, project team members, and stakeholders; develop decision making documents; and assess and understand complex business processes and customer requirements to ensure new technologies, architectures, and security products will meet their needs. 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.

RESPONSIBILITY FOR DECISIONS AND CONSEQUENCES OF ERROR

The incumbent will make recommendations concerning the security, integrity and availability of Department information and information systems. The effect of those recommendations will impact the efficient and effective operation and performance of IT and the Departmental operations. Recommendations will influence Department information security policy. The incumbent must exercise good judgment, analyze problems, and take appropriate action. Poor decisions or recommendations could result in significant losses of departmental efficiencies through unnecessary delays, loss of data, equipment damage, loss of employee

POSITION DUTY STATEMENT

DOT PM-0924 (REV 01/2025)

productivity, and user dissatisfaction.

PUBLIC AND INTERNAL CONTACTS

The incumbent will be in contact with members of IT, Department staff and Executive Management staff. On occasion, the ITM I will be in contact with other cybersecurity related agencies internal and external to State of California governmental offices. External contacts may include international, national, State and private sector information security contacts, Business, Transportation & Housing Agency, the Governor's Office and other Legislative Offices. The incumbent may represent the Department at various conferences and seminars and will also have occasional contact with contractors/vendors and members of the public-at-large.

PHYSICAL, MENTAL, AND EMOTIONAL REQUIREMENTS

The incumbent may be required to sit for long periods of time using a keyboard, video display terminal and telephone and may be required to lift and move supplies and equipment from one location to another. The incumbent must be able to walk between multiple State buildings and have a thorough knowledge of Caltrans building locations. This is a fast-paced job with a lot of deadlines. Thus, the incumbent in this position will be required to multi-task, be open to change, adapt to changes in priorities and policies, and to complete tasks or projects with short notice. The incumbent must be able to sustain mental activity needed for problem solving which includes reading, writing, analyzing, understanding, interpreting, consulting, developing alternatives, drawing sound conclusions, and recommending, implementing and evaluating solutions. The incumbent must be able to exercise sufficient control over emotions to gain and maintain the confidence and respect of others, recognizing and acknowledging emotionally charged issues or problems and responding appropriately to them.

WORK ENVIRONMENT

This position may be eligible for telework. The amount of telework is at the discretion of the Department and based on Caltrans's evolving telework policy. Caltrans supports telework, recognizing that in-person attendance may be required based on operational needs. Employees are expected to be able to report to their worksites with minimum notification if an urgent need arises. The selected candidate will be required to commute to the headquartered location as needed to meet operational needs. Business travel may be required, and reimbursement considers an employee's designated headquartered location, primary residence, and may be subject to CalHR regulations or applicable bargaining unit contract provisions. All commute expenses to the headquartered location will be the responsibility of the selected candidate.

If not working remotely, the employee will work in a climate-controlled office under artificial lighting using a personal computer. The employee may be required to work for extended periods of time in a computer room that maintains an approximate temperature of 70 degrees.

The employee may be required to travel. When available, a State vehicle will be provided. Possession of a valid driver's license is required when operating a State owned or leased vehicle. If the employee utilizes their own personal vehicle, they may be reimbursed for travel expenses.

Some weekend or after-hours may be required. The employee must carry a cell phone and respond to calls after hours.

POSITION DUTY STATEMENT

DOT PM-0924 (REV 01/2025)

I have read, understand and can perform the duties listed above. (If you believe you may require reasonable accommodation, please discuss this with your hiring supervisor. If you are unsure whether you require reasonable accommodation, inform the hiring supervisor who will discuss your concerns with the Reasonable Accommodation Coordinator.)

I agree that by providing my electronic signature for this form, I agree to conduct business transactions by electronic means and that my electronic signature is the legal binding equivalent to my handwritten signature. I hereby agree that my electronic signature represents my execution or authentication of this form, and my intent to be bound by it.

EMPLOYEE (Print)

EMPLOYEE (Signature)	DATE
----------------------	------

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

SUPERVISOR (Print)

SUPERVISOR (Signature)	DATE
------------------------	------