Duty Statement

Classification: **Information Technology Manager I** **JC-371824**

Position Number: **275-817-1405-005** HCM#: **2137**

Branch/Section: **Information Security Office / Governance, Risk, and Compliance**

Location: **Sacramento, CA** Telework: Office-centered

Working Title: **Governance, Risk, and Compliance Manager** Effective Date: **May 1, 2023**

Collective Bargaining Identifier (CBID): **M01** Supervision Exercised: ☒ **Yes** ☐ **No**

The Information Security Office (ISOF) leads the organization's effort to safeguard data, IT Systems, and business processes from cyber threats. ISOF's primary responsibilities include identification, elevation and tracking of cybersecurity risks; operating several critical common controls to protect and detect potential cybersecurity incidents; establishing security standards and guidelines to meet organization and regulatory requirements; providing consultation and cybersecurity awareness training.

Under the general direction of the Chief Information Security Officer (CISO), the Information Technology Manager I (IT MGR I) leads the Governance, Risk, and Compliance (GRC) team. The IT MGR I is responsible for establishing and maintaining the CalPERS information security GRC program. This includes the implementation and maintenance of policies, as well as a comprehensive controls framework for third-party risk management. The IT MGR I will work across divisions, provide oversight and ensure effective implementation of practices in compliance with regulatory and policy requirements.

Essential Functions

30% Responsible for implementing an overall CalPERS data protection framework including developing, reviewing, and updating Information Technology (IT) and information security policies, standards, guidelines, and baseline to protect CalPERS data and systems. Partner with data stewards and other functional leaders, IT leaders and staff to leverage technologies and processes to develop and maintain a comprehensive data governance program. This includes control design and implementation guides, training, continuous monitoring, alerting, and reporting. Coordinate the development and implementation of an enterprise-wide information security training and awareness program.

25% Develop and manage an information security risk management program including the development, evaluation, and adherence to multiple areas of practice. Develop a risk strategy that identifies and classifies risks, defines appropriate tolerances, prioritizes mitigation activities, and measures risk levels using the CMMI Cyber Maturity / NIST CSF Framework. Establish and oversee a formal risk analysis and self-assessments program for various information services, systems, processes and recognized industry standards. Identify, assess, manage, and track remediation of risks related to IT infrastructure, applications, platforms and suppliers and drive explicit requirements and timelines in all environments. Develop strong relationships with external audit and key stakeholders to ensure risk management oversight is understood, managed appropriately and current with all standards, guidelines, and regulations that are applicable

25% Oversees all one-time and ongoing activities related to the development, implementation, and maintenance of the CalPERS Health information and privacy program, in accordance with applicable federal and state laws. Manages, organizes, directs, and coordinates the activities of staff within the Information Security Health

Insurance Portability Accountability Act (HIPAA) and Privacy section. Assesses methods and procedures used to store and transmit personal health information (PHI); identify security or other compliance risks and researches and recommends improvements. Maintains policies and procedures related to PHI access and use; ensures strict adherence by all staff with access to PHI.

15% Develop, monitor, maintain, evolve, and drive delivery of CalPERS's Third-Party Risk Management (TPRM) program, coordinating activities across multiple divisions. Define and establish program governance structures to support successful delivery and manage TRPM program risks. Ensures the TPRM program is in compliance with all relevant third-party laws and regulations; establish regulatory scanning processes to ensure adherence with relevant TPRM related regulations on an ongoing basis. Assess alignment of TPRM standards/practices with regulatory requirements and established and emerging industry practices. Provide ongoing oversight on CalPERS TPRM practices through defined, repeatable procedures. Review procedures for completeness, compliance and adequacy on an ongoing basis. Ensure strong management of TPRM issues, risk acceptances, and exceptions is in place. Provide ongoing visibility into issues, risk acceptances, and exceptions by establishing ongoing reporting.

5% Participate as needed in special ad-hoc committees, projects, and other IT initiatives. Perform special assignments as required.

Working Conditions

- Office environment (three days minimum), telework environment (two days maximum)

Conduct, Attendance, and Performance Expectations

- Ability to maintain consistent attendance
- Ability to demonstrate punctuality, initiative, and dependability
- Ability to model and support CalPERS Core Values (Integrity, Accountability, Respect, Openness, Quality, and Balance)
- Ability to model CalPERS Competencies and demonstrate proficiency in; Collaboration, Leading People, Leading Change, Driving Results, Business Acumen, Communication, and Leading Self

I have read and understood the duties and essential functions of the position and can perform these duties with or without reasonable accommodation.

Employee Name (Print):

Employee Signature: ______________________________ **Date**:

I certify that the above accurately represent the duties of the position.

Supervisor Signature: ______________________________ **Date**: