CalPERS

Duty Statement

Classification: **Information Technology Manager II**

Position Number: **275-817-1406-001**

HCM#: **1204**

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

Location: **Sacramento, CA**

Working Title: **Assistant Division Chief**

Effective Date: **January 20, 2026**

Collective Bargaining Identifier (CBID): **M01**

Supervision Exercised: ☒ **Yes** ☐ **No**

Telework: ☒ **Office-Centered** ☐ **Remote-Centered** ☐ **Not Eligible**

The Information Security Office (ISOF) leads the organization's efforts to safeguard data, information technology systems, and business processes from cyber threats and privacy risks. ISOF's primary responsibilities include the identification, elevation, and tracking of cybersecurity, privacy, and regulatory risks; operating and overseeing critical common controls to protect and detect potential security and privacy incidents; establishing security, privacy, and risk management standards to meet organizational and regulatory requirements (including HIPAA); and providing enterprise-wide consultation and security and privacy awareness training.

Under the administrative direction of the Chief Information Security Officer (CISO), the Information Technology Manager II (IT MGR II) is responsible for the day-to-day management and oversight of the Governance, Risk, and Compliance (GRC), HIPAA and Privacy, and Security Awareness programs within ISOF. This position provides leadership, executive support, and strategic and tactical direction for security governance, enterprise risk management, regulatory compliance (including HIPAA and privacy obligations), and organization-wide security and privacy awareness initiatives.

The IT MGR II directly supervises two Information Technology Manager I (IT MGR I) positions: the Governance and Risk Manager, and the Privacy Program Officer. The Privacy Program Officer is responsible for the HIPAA and Privacy Program and for overseeing security and privacy awareness activities. Through these managers, the IT MGR II ensures effective program execution, staff performance management, and alignment of governance, risk, privacy, and awareness functions with CalPERS' strategic objectives.

As a business enabler, the IT MGR II ensures business decisions are supported—not obstructed—by cybersecurity and privacy requirements and are informed by sound risk-based principles in alignment with CalPERS policies, legal obligations, and strategic goals. The IT MGR II leads a business-supporting team focused on policy, compliance, risk analysis, HIPAA and privacy assurance, security and privacy awareness, and audit readiness. The IT MGR II collaborates closely with technical staff across the organization, including software developers, systems engineers, and cybersecurity teams, but does not have direct supervisory responsibility over ISOF security engineering or security operations teams.

The IT MGR II is expected to be a strong communicator with demonstrated business acumen, capable of working effectively with executive leadership and operational stakeholders. This role requires frequent interaction with C-level executives, legal and compliance partners, third parties, regulators, and audit committees. The IT MGR II fosters a culture in which staff feel valued, supported, and challenged while maintaining sustainable workloads. Key personnel responsibilities include recruitment, performance management, career development, and retention for staff within the GRC, HIPAA and Privacy, and awareness functions. A solid technical and regulatory foundation is required to understand emerging threats, privacy risks, compliance obligations, and control frameworks.

Essential Functions

Regular and consistent attendance in the office at least three days a week is required for teamwork, in-person collaboration, personal interactions with members, stakeholders, and other team members, as well as cross-functional communications within CalPERS. In-person coordination promotes innovation, engagement, and alignment across teams and enables timely discussions, mentoring, and strategic planning.

40% [1] Onsite and virtually, provide recommendations to the CISO on information security, privacy, and HIPAA standards and best practices for information technology initiatives. Assist the CISO in overseeing the effectiveness of the security governance, enterprise risk management, HIPAA and Privacy, and security and privacy awareness programs. Supervise IT MGR I staff to ensure consistent execution of GRC, privacy, and awareness responsibilities. Coordinate with business partners to resolve complex or sensitive policy, privacy, and compliance issues. Provide guidance to staff at all levels on cybersecurity risk, HIPAA and privacy requirements, compliance obligations, and awareness needs. Develop and implement integrated GRC, HIPAA and Privacy, and awareness programs aligned with business objectives. Define and track metrics to measure program effectiveness and maturity. Participate in budget planning to ensure adequate resources for governance, privacy, and awareness priorities.

30% Onsite and virtually, oversee the development, implementation, and maintenance of information security, privacy, and HIPAA-related policies, standards, and control frameworks. Ensure cybersecurity, privacy, and regulatory risks are identified, documented, tracked, and communicated to appropriate risk owners and governance bodies. Provide management oversight and coordination for privacy and security incident response activities in collaboration with technical leads, Legal, and business units, including documentation, lessons learned, and corrective action tracking. Support disaster recovery and business continuity planning from a risk, compliance, and policy perspective, promoting risk-informed decision-making and adherence to regulatory requirements.

30% Onsite and virtually, ensure timely, accurate, and well-coordinated responses to internal and external audits, assessments, and regulatory inquiries, including those related to HIPAA and privacy. Collaborate with Legal, Compliance, Enterprise Risk, Internal Audit, and Human Resources to develop, implement, and maintain security- and privacy-related policies and procedures. Maintain effective working relationships with external regulators, oversight entities, and law enforcement as appropriate. Establish and sustain strong partnerships with business units to support risk assessments, privacy impact analyses, remediation tracking, and the adoption of business-aligned security and privacy practices. Represent CalPERS in statewide, interagency, or industry governance, risk, security, and privacy forums as assigned. Perform other duties as assigned.

Working Conditions

- [1] This position is designated as office-centered and works primarily onsite at the Sacramento, CA - Headquarters at least three weekdays.
- Workstation is located in a standard multi-level office building accessible by stairs and elevator, with artificial light, height-adjustable desk, and adjustable office chair.
- Prolonged reading and typing on a laptop or keyboard and monitor.

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**: