



Duty Statement

Classification: **Information Technology Manager I**

Position Number: **275-817-1405-006**

HCM#: **1220** **JC-376187**

Branch/Section: **Information Security Office/Fraud/Incident Management**

Location: **Sacramento, CA**

Telework: Office-centered

Working Title: **Fraud Prevention Program 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, Information Technology (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), Fraud Prevention Program Manager, implements and coordinates fraud prevention, mitigation, and investigation activities and functions, such as identifying high-risk transactions, emerging threats, researching, and resolving suspicious activities, performing investigations, implementing appropriate controls, and recovering funds. The IT MGR I leads a team of analysts who participate in the intake, triage, risk and exposure analysis, detection, investigation, and control activities to mitigate the threat of fraud. The IT MGR I may directly participate in the review and disposition of activity with their staff. Activity may include, but is not limited to, access and authentication through various channels such as web and phone, and paper to pension, health, and employer CalPERS delivered services.

Essential Functions

- 40% Maintain the overall health of the organization's fraud prevention program by identifying, assessing, and mitigating operational and transactional risks by developing and monitoring risk-based programs based on organizational risk appetite(s). Keep abreast of pending/regulatory issues by tracking and monitoring the fraud landscape, analyzing, and reporting trends impacting the organization and the membership and providing insights and analysis to leadership and governing committees. Measure the effectiveness and efficiency of controls and act to continuously improve Key Performance Indicators (KPIs) and overall organization and process performance by embedding and automating processes in core products, fraud prevention tools, and operational procedures by working with key stakeholders.
- 30% Manage and coordinate fraud prevention, mitigation, and investigation activities and functions, such as identifying high-risk transactions and emerging threats, researching, and resolving suspicious activities, performing investigations, implementing appropriate controls, and recovering funds. Implement fraud detection, prevention, and mitigation analytics, tools, techniques, and controls, and recommend correction items in response to loss or high-risk events. Perform investigations and collaborate with appropriate business partners and local, state, and federal authorities. Develop, update, and implement, as appropriate, fraud mitigation and investigation procedures and educational materials for internal and external customers. Provide training to and share knowledge with staff, management, and other departments on effective fraud prevention practices. Act as the escalation point of contact for fraud mitigation issues, problems, and

questions directly related to fraud mitigation and services. Assist members and staff with resolving difficult or complex issues with quick turnaround and accuracy. Work, as needed, with account holders, third parties, and law enforcement. Notify and communicate appropriate updates to management, as needed.

- 30% Ensure adherence to regulatory, organizational, and team service level agreements (SLA's). Implement and/or assist in developing action plans for detecting and responding to fraudulent activities against the organization. Partner with key fraud stakeholders and business partners through project involvement, important topic presentations, and operational oversight. Ensure the Fraud Detection Standard Operation Procedures (SOP) and Fraud Response SOP are appropriately documented and are compliant with regulatory requirements, meeting or exceed industry best practices. 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:**