YOUR EFFORTS WILL MAKE FI$Cal A SUCCESS
DUTY STATEMENT

CLASSIFICATION TITLE Information Technology Specialist II	**DIVISION NAME** Information Technology Division, Enterprise Security Services Office, Information Systems Security Management Section
WORKING TITLE Senior Compliance Specialist	**POSITION NUMBER** 333-350-1414-031
EMPLOYEE NAME Vacant	**EFFECTIVE DATE** TBD

You are a valued member of the Department of FI$Cal. You are expected to work cooperatively with team members and others to provide the highest level of service possible. Your creativity and productivity is encouraged. Your efforts to treat others fairly, honestly and with respect are important to everyone who works with you.

GENERAL STATEMENT
Under the general direction of the Information Technology Manager I, the Information Technology Specialist II (ITS II) works independently and collaboratively on multiple waves of analysis, design, development, implementation, operations, and maintenance of software systems and the Financial Information System for California (FI$Cal) system. The ITS II provides technical and analytical leadership in the areas of information security architecture, policy, standards, governance, risk and compliance management.

The duties for this position are focused in the information security engineering domain, however, work may be assigned in the other domains as needed.

SUPERVISION RECEIVED
The Information Technology Specialist II reports directly to the Information Technology Manager I of the Information Systems Security Management Section.

SUPERVISION EXERCISED
None

ESSENTIAL FUNCTIONS

The incumbent must be able to perform the essential functions with or without reasonable accommodation. Specific duties include, but are not limited to, the following:

% OF TIME	ESSENTIAL FUNCTIONS
40%	**Information Security Management** • Develop and maintain up-to-date FI$Cal information system security plans, procedures, guidelines and forms, for timely updates of the annual reviews and audits. • Develop and verify security solutions and technical artifacts for FI$Cal IT systems and platforms • Monitor and assess security controls in alignment of SAM including National Institute of Standards and Technology (NIST) SP 800-53 (Security and Privacy Controls for Federal Information Systems and Organizations) for FI$Cal solutions on an ongoing basis, document changes, conduct security impact analyses and create reports for system security statuses. • Lead ongoing assessment efforts of all security controls in place and ensure their continued effectiveness. • Lead state staff in custom code reviews in accordance with federal/state/industry best practice methodologies such as NIST SP 800-28 (Guidelines on Active Content and Mobile Code). • Analyze business impact and exposure based on threats, risks and vulnerabilities for new FI$Cal requirements and establish traceability for completeness to ensure security requirements are met. • Verify new technology services and solutions meet standards for secure solutions and adhere to State Administrative Manual (SAM) requirements. • Verify hosted vendor services and internal solutions are reviewed and updated annually for continuity and recovery plans that outline and address the proper processes, technologies, and techniques to prepare for, mitigate, respond to security incidents and ensure operational continuity. • Analyze the effectiveness of the backup and recovery of data, programs, and services.
35%	**Information Security Governance, Risk, and Compliance Management** • Lead risk management processes (e.g., methods for assessing and mitigating risk).

	• Analyze and recognize changes in laws, policies or regulations that impact the privacy or security of confidential information for the FI$Cal enterprise. • Develop and update Memorandum of Understanding (MOU) between FI$Cal and each participating state entity in each release, in coordination with the FI$Cal legal. • Develop policies and procedures concerning information security and privacy to ensure compliance with SAM 5300 (Information Security), and NIST SP 800-53. • Lead Technology Team tasks on data classification and protection for each release, including the confidential gathering, tabulation, analysis, and reporting of state entities' inventory of data elements and data classification for all applicable FI$Cal Enterprise Resource Planning (ERP) modules. • Conduct in-depth evaluations of all roles in the FI$Cal System and report on compliance of these roles with federal and state requirements with respect to authentication per the NIST SP 800-53. • Lead and train Enterprise Security Service (ESS) staff in the initiation, planning, analysis, design, development, testing, implementation, configuration, and maintenance of security tools (hardware/software) and processes. • Lead the identification and classification of all records and identification of ownership responsibilities for all records, files and databases to ensure the integrity and security of agency information assets.
25%	**Collaboration and Coordination** • Coordinate and oversee system/software deployments and patching, ERP access activities, vulnerability scanning, and penetration testing to ensure successful progress and execution. • Oversee contractors that conduct annual independent security assessments in compliance with SAM 5300 (Information Security) and NIST SP 800-53. • Lead state guidance and reviews of contractors' Deliverable Expectation Documents, deliverables, and milestones. • Act as liaison with the System Integrator's Technical Architecture lead, Database and System Administration leads, and Application Security leads to ensure the design, development, and implementation of the FI$Cal System fully meets all enterprise security related requirements. • Facilitate and coordinate security audits to test for effectiveness of all administrative, technical, and physical security controls required for SAM and NIST SP 800-53. • Lead oversight efforts for the implementation and evaluation of security controls.

	• Analyze and report on security technology industry and market trends as well as determine their potential impact on the enterprise. • Promote the security enterprise architecture process, outcomes and results to the organization, including the enterprise's IT and industry leaders, through applying Sherwood Applied Business Security Architecture (SABSA) methodology, California Enterprise Architecture Framework (CEAF), etc. • Lead the identification and analysis of enterprise business security drivers to derive enterprise business, information, technical and solution architecture requirements. • Interface with all FI$Cal participating state entities' Information Security Offices as well as the state's Chief Information Security Office on matters related, but not limited, to data classification and protection, security risk and privacy assessments, security incidents and reporting.
% OF TIME	**MARGINAL FUNCTIONS**
5%	• Perform other related duties as required to fulfill FI$Cal's mission, goals and objectives. Additional duties may include, but are not limited to, assisting where needed within the team/unit, which may include special assignments.

KNOWLEDGE AND ABILITIES

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.

SPECIAL REQUIREMENTS

The incumbent will use tact and interpersonal skills to develop constructive and cooperative, working relationships with others, e.g., stakeholders, customers, management, peers, etc., to facilitate communication to improve the work environment and increase productivity. **Fingerprinting and background check are required.**

WORKING CONDITIONS

The incumbent may need to be on-site to carry out their duties. This position requires the ability to work under pressure to meet deadlines and may require excess hours to be worked. The incumbent should be available to travel as needed and is expected to perform functions and duties under the guidance of the Department of FI$Cal's core values. The incumbent provides back-up, as necessary, to ensure continuity of departmental activities.

This position requires prolonged sitting in an office-setting environment with the use of a telephone and personal computer. This position requires daily use of a copier, telephone, computer and general office equipment, as needed. This position may require the use of a hand-cart to transport documents and/or equipment over 20 pounds (i.e., laptop, computer, projector, reference manuals, solicitation documents, etc.). The incumbent must demonstrate a commitment to maintain a working environment free from discrimination and sexual harassment. The incumbent must maintain regular, consistent, predictable attendance, maintain good working habits and adhere to all policies and procedures.

SIGNATURES

I have read and understand the duties listed above and I can perform these duties with or without reasonable accommodation. (If you believe reasonable accommodation is necessary, discuss your concerns with the hiring supervisor. If unsure of a need for reasonable accommodation, inform the hiring supervisor, who will discuss your concerns with the assigned HR analyst.)

_____

Employee Signature Date

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

_____

Hiring Manager Signature Date

HR Analyst _AR__

Date Revised: 12/27/24