

YOUR EFFORTS WILL MAKE FI\$Cal A SUCCESS DUTY STATEMENT

CLASSIFICATION TITLE Information Technology Specialist I	DIVISION NAME Information Technology Division
WORKING TITLE Governance Risk and Compliance (GRC) management Specialist	OFFICE/SECTION/UNIT Enterprise Security Services Office, Information Systems Security Management Section
EMPLOYEE NAME VACANT	POSITION NUMBER 333-350-1402-043

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 direction of the Information Technology Manager (ITM) I, Enterprise Security Services Office (ESSO), Information Systems Security Management Section (ISSMS), the Information Technology Specialist (ITS) I will serve as a Governance Risk and Compliance (GRC) management specialist, to manage audit processes, liaison with information security auditors, develop and oversee security policies, guidelines, and standards. The incumbent will ensure compliance with industry standards, state and federal security requirements. The incumbent will assist with the collection and review of documents for audits and assessments, will ensure that the procedures are in alignment with FI\$Cal security policies and will provide guidance on the development of procedures within various units of the department.

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

Reports directly to the ITM I, ISSMS.

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:

<u>% OF TIME</u>	<u>ESSENTIAL FUNCTIONS</u>
35%	Information Security Governance, Risk, and Compliance (GRC) Management & Collaboration • Analyze audit reports and findings, develop plan of action to address compliance exceptions and to mitigate risks. • Execute risk management processes (e.g., methods for assessing and mitigating risk). • 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 National Institute of Standards and Technology (NIST) SP 800-53. • 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. • Support the organization's privacy compliance program, working closely with the other departmental units, Chief Information Security Officer, Chief Information Officer, legal counsel and the business units. • Collaborate with stakeholders to ensure policy awareness and compliance. Participate in the review of the System Security Plan to assure implementation of sound security principles and adherence to security requirements as outlined in NIST, Federal Information Protection Standards (FIPS), Statewide Information Management Manual (SIMM) and State Administrative Manual (SAM).
20%	Managing the GRC audit process • Manage audit processes, all security governance and compliance business processes. • Liaison with information security auditors and collaborate with internal stakeholders with respect to audit. • Carry out internal audits, collect evidences, and make recommendations. • Assemble, organize and otherwise prepare documents for audits and assessments.

20%	Policy & Procedure Review and Development • Review and assess current procedures impacting IT Security within the department; collaborate with FI\$Cal's Information Technology Division (ITD) and various other units throughout the department to ensure procedures are in alignment with FI\$Cal policies and industry best practices. • Research industry IT Security practices and make recommendations to management on risk mitigation for departmental processes. • Monitor and ensure compliance with the rigorous application of cyber policies, principles, and practices. • Ensure that cyber workforce management policies and processes comply with legal and organizational requirements.
20%	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. • Monitor and assess security controls in alignment of SAM including NIST SP 800-53 for FI\$Cal solutions on an ongoing basis, document changes, conduct security impact analyses and create reports for system security statuses. • Carryout assessment of all security controls in place and ensure their continued effectiveness. • 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 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.
% 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

All knowledge and abilities of the Information Technology Associate classification; and

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.

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.

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 FISCal'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

H/R Analyst PGR

Date Revised: 08/14/2026

YOUR EFFORTS WILL MAKE FI\$Cal A SUCCESS

DUTY STATEMENT

CLASSIFICATION TITLE	DIVISION NAME
Information Technology Associate	Information Technology Division
WORKING TITLE	OFFICE/SECTION/UNIT
Governance Risk and Compliance (GRC) management Associate	Enterprise Security Services Office, Information Systems Security Management Section
EMPLOYEE NAME	POSITION NUMBER
VACANT	333-350-1401-XXX

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 supervision of the Information Technology Manager (ITM) I, Enterprise Security Services Office (ESSO), Information Systems Security Management Section (ISSMS), the Information Technology Associate (ITA) will serve as a Governance Risk and Compliance (GRC) management Associate, to carry out audit related tasks, liaison with information security auditors, and assist in development of security policies, guidelines, and standards. The incumbent will assist with the collection and review of documents for audits, assessments and compliance with industry standards, state and federal security requirements. The incumbent will ensure that the procedures are in alignment with FI\$Cal security policies and will provide guidance on the development of procedures within various units of the department.

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

Reports directly to the ITM I, ISSMS.

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:

<u>% OF TIME</u>	<u>ESSENTIAL FUNCTIONS</u>
35%	Information Security Governance, Risk, and Compliance (GRC) Management & Collaboration • Analyze audit reports and findings, develop plan of action to address compliance exceptions and to mitigate risks. • Execute risk management processes (e.g., methods for assessing and mitigating risk). • Execute tasks with respect to all security governance and compliance business processes. • Collaborate with stakeholders to ensure policy awareness and compliance.
35%	Participating in the GRC audit process • Execute security governance and compliance tasks associated with the audit processes. • Liaison with information security auditors and collaborate with internal stakeholders with respect to audit. • Support internal audits and collect evidence to make recommendations. • Assemble, organize and otherwise prepare documents for audits and assessments
25%	Policy & Procedure Review and Development • Review and assess current procedures impacting IT Security within the department; collaborate with FI\$Cal Information Technology Division (ITD) and various other units throughout the department to ensure procedures are in alignment with FI\$Cal policies and industry best practices. • Monitor and make recommendations on the rigorous application of cyber policies, principles, and practices. • Ensure that cyber workforce management policies and processes comply with legal and organizational requirements.
<u>% OF TIME</u>	<u>MARGINAL FUNCTIONS</u>
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

All knowledge and abilities of the Information Technology Technician classification; and

Knowledge of: Principles, techniques, and procedures related to the delivery of information technology services; the System Development Lifecycle including the associated methodologies, tools, and processes; the organization's business processes and procedures; education tools and techniques; performance monitoring tools and techniques; and data administration techniques and best practices.

Ability to: Use initiative; act independently with flexibility and tact; use logic and reasoning to identify the strengths and weaknesses of alternative solutions, conclusions or approaches to problems; perform technical analysis of proposed technology solutions; comprehend technical documents to interpret specifications, system implementations, capabilities, interdependencies, and compatibilities; serve as a technical liaison; develop and effectively utilize all available resources; develop end-user training materials; and gather data to perform statistical analysis and report outcomes.

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 FISCAL'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

H/R Analyst PGR

Date Revised: 08/11/2026