LOS ANGELES UNIFIED SCHOOL DISTRICT
PERSONNEL COMMISSION

CLASS DESCRIPTION
CLASS CODE 4859
Management-District

INFORMATION SECURITY COMPLIANCE ANALYST

DEFINITION

Plans and conducts analysis of all IT security-related compliance activities within the Information Technology Division's (ITD) control environment including information security, data privacy, IT controls over financial reporting, contracts, business continuity, identity management, user access and data integrity.

TYPICAL DUTIES

- Maintains a compliance control program and use it to continuously identify, document, assess, monitor, test, and assign compliance controls within ITD's compliance control environment.
- Liaises with internal and external entities in support of IT compliance-related documentation requests, reports, corrective actions, interpretations, assurances, investigations, contract reviews, projects, incident response, and other IT actions subject to compliance requirements.
- Collects, analyzes, and tracks IT compliance data from various functional units in a relational database in order to develop and maintain dashboards that provide visibility into the operational effectiveness of the compliance program.
- Creates IT compliance training and awareness content and train stakeholders on their responsibilities related to their role, and certifies their compliance.
- Analyzes and compares the District's IT security policies, procedures, and standards to the District's actual practices to identify any areas of noncompliance and work across functional lines to communicate findings and assign appropriate controls to business owners.
- Evaluates essential IT contracts and agreements to document non-compliance with terms and conditions that may negatively affect the confidentiality, integrity or availability of IT services and assets.
- Monitors, assesses, and reports compliance with internal controls over financial reporting including but, not limited to segregation of duties, authorizations, access control, and general IT controls related to the confidentiality, integrity, and availability of financial data.
- Inventories, analyzes, and evaluates new, current and proposed IT-related regulations, laws, Board Rules, internal policies, procedures, practices, security standards, IT assets, and any affected parties to determine compliance requirements and impacts to the District.
- Drafts new and maintains existing IT-related policies and their controls based on relevant changes in the IT control environment and risk assessments.
- Maintains an annual schedule of IT security policy and procedure reviews and submit for approval.
- Performs other duties as assigned.

DISTINGUISHING CHARACTERISTICS AMONG RELATED CLASSES

An Information Security Compliance Analyst conducts comprehensive assessments of IT security operations to ensure that reasonable measures are taken to comply with applicable laws, regulations, external security frameworks, and Board Rules and ITD policies.

The Information Security Risk Manager conducts comprehensive assessments of IT assets and services to identify and manage risks that may negatively impact the delivery of IT services and interrupt District operations.

An IT Security Analyst I performs a variety of technical assignments in an effort to protect information assets by testing and evaluating systems; identify and document vulnerabilities, and raises awareness of information security initiatives and practices.

SUPERVISION

General supervision is received from the Information Security Risk Manager. Work direction may be exercised over lower level personnel.

CLASS QUALIFICATIONS

Knowledge of:

- One or more of the following concepts, procedures and controls relating to ISO 27001, ISO 27002, ISO 22301, ITIL, NIST 800-53, COBIT 5, COSO Internal Controls, or other industry accepted information security control frameworks
- National and California laws, regulations, and best practices relevant to information security, public education, auditing, contract administration, and IT controls for financial reporting
- Basic principles and procedures of cost analysis and control, budgeting accounting, auditing, contract law and public purchasing
- Principles and practices of business and public administration particularly as related to organization and management, planning, research, budgetary and fiscal practices, material acquisition, purchasing, and contracting
- Methods, procedures and techniques of research, record development and management, data collection, statistical and financial analysis research and report presentation
- Data processing systems and programs as they relate to purchasing and finance activities
- Information Technology environments, enterprise resource planning and auditing procedures
- Enterprise Risk Management
- Performance Management and Performance Measurement systems
- Microsoft Windows operating system and relevant software
- Microsoft Office applications including but not limited to Word, Excel, PowerPoint, and Visio

Ability to:

- Understand, interpret, and apply laws, rules, regulations, policies, and procedures and develop appropriate internal controls.
- Perform IT compliance assessments and develop and submit compliance reports.
- Apply IT-related knowledge and experience in solving compliance issues and exercise good judgment in making decisions
- Interpret and analyze audit results and findings and describes the overall impact to subject matter experts
- Communicate effectively both verbally and in writing
- Problem solve and work within established timeframes to deliver timely results with minimal supervision
- Establish and maintain effective working relationship with District personnel and external stakeholders
- Conduct meetings and give effective presentations
- Work with a wide variety of financial, contract, and computer systems
- Maintain confidentiality, impartiality and objectivity

ENTRANCE QUALIFICATIONS

Education:

Graduation from a recognized college or university with a bachelor's degree in legal studies, computer science, information systems, business or public administration, or a related field.

Experience:

Two years of experience performing compliance assessments in an IT environment for a large organization.

Special:

Certified Authorization Professional (CAP), Certified Security Compliance Specialist (CSCS), Certified Information Systems Auditor (CISA), Certified ISO/IEC 27001 Lead Implementer certification, or equivalent certifications are preferable.
A valid California Driver License.
Use of an automobile.

This class description is not a complete statement of essential functions, responsibilities, or requirements. Entrance requirements are representative of the minimum level of knowledge, skill, and/or abilities. To the extent permitted by law, management retains the discretion to add or change typical duties of a position at any time, as long as such addition or change is reasonably related to existing duties.

New Class
05-14-18
PJO