LOS ANGELES UNIFIED SCHOOL DISTRICT
PERSONNEL COMMISSION

CLASS DESCRIPTION
CLASS CODE 4786
Management-District

INFORMATION SECURITY RISK MANAGER

DEFINITION

Establishes and maintains the District's overall asset-based IT security risk management program to ensure that IT systems and information assets are adequately protected and is responsible for all IT-related risk assessment processes and identification activities.

TYPICAL DUTIES

Manage all the risk-related activities of the Information Technology Division including the analysis, identification, and estimation of IT risks and the development, planning, testing, and documenting of remediation measures.
Develops and conducts IT risk assessment and treatment plans with recommended for security assessments, business performance, and expected costs/benefits.
Benchmarks the IT risk management practices of other school Districts and maintain an up-to-date understanding of industry best practices, and monitor the legal and regulatory environment for developments that could require changes to the District's established IT policies and practices.
Coordinates with the IT Project Management Office to filter enterprise IT risks from the tactical daily project risks and verifies that they are properly quantified, prioritized, documented, treated, monitored and incorporated into the IT risk management program
Creates and maintains a centralized IT risk register to electronically store and manage all identified risks and relevant attributes to support the IT risk management process.
Develops, implements, and applies appropriate methods and processes to assess the likelihood and level of consequences that losses of confidentiality, integrity and availability of IT assets may have on District operations.
Works and negotiates with risk owners on deficiencies identified in monitoring reviews, internal IT risk assessments, automated assessments, and internal/external audits to ensure that that effective and appropriate IT risk remediation measures have been taken.
Monitors and reviews new IT assets, new legal and regulatory changes, total cost of ownership, changes to IT asset values, new unassessed security threats and new vulnerabilities to identify any changes in the context of the overall IT risk posture of the District.
Responds to internal and external audit request for information related to IT security risk management.
Develops a risk training program and conducts IT risk analysis trainings for IT project managers and other stakeholders.
Identifies risk of potential losses related to IT assets,
Performs other duties as assigned.

DISTINGUISHING CHARACTERISTICS AMONG RELATED CLASSES

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 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 Director of IT, Security is responsible for the development and implementation of computer network security procedures for the information services function.

SUPERVISION

General supervision is received from the Director of IT, Security. Supervision is exercised over the Information Security Compliance Analyst and lower level IT staff.

CLASS QUALIFICATIONS

Knowledge of:

- Broad range of IT security and risk management frameworks such as ISO 27005, RiskIT (ISACA), NIST 800-37, ISO 31000, CoBIT 5 for Risk, Cobit 5 for Information Security, COSO, ISO 27001, ISO 27002, and NIST 800-53, and ITIL.
- Laws, regulations, practices, and procedures relevant to California public education, strategic IT risks, IT controls over financial reporting, IT auditing, and IT contract administration.
- Broad IT risk-related disciplines, including IT governance, information security, business continuity, data privacy, regulatory compliance, and IT operations.
- Basic principles and procedures of cost analysis and control, budgeting accounting, auditing, contract law and public purchasing
- Fundamentals of Information Technology environments and auditing procedures and enterprise risk management
- Performance management and performance measurement systems

Ability to:

- Analyze and interpret pertinent laws, rules, regulations, accounting and technical data, written materials, oral communications, and contracts
- Understand, interpret, and apply laws, rules, regulations, policies, and procedures
- Interpret and analyze audit results and findings and describes the overall impact to subject matter experts
- Develop and implement goals, objectives, policies, procedures, and internal controls
- Communicate effectively both verbally and in writing to technical and non-technical audiences
- Problem solve and work within established timeframes to deliver timely results with minimal supervision
- Formulate innovative recommendations for process improvement and enhance organizational effectiveness
- 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
- Supervise, train, and evaluate the work of reporting personnel

ENTRANCE QUALIFICATIONS

Education:

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

Experience:

Four years of professional-level experience in conducting risk reviews and assessments, and developing treatment plans and reports for a large organization. One year of the above

experience must have included designing and implementing an asset-based IT risk management program. Supervisory experience is preferable.

Special:

A Certified Risk and Information Systems Control (CRISC), PMI Risk Management Professional (PMI-RMP), Certified Authorization Professional (CAP), GRC Professional (GRCP), RIMS-Certified Risk Management Professional (RIMS-CRMP), or equivalent certification is preferred.
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