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 risk and IT continuity management programs to ensure that IT systems and information assets are adequately protected and there is minimum business impact in the event of an IT service interruption.

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.
- Manage all the IT continuity related activates based on industry best practices and a broad range of IT continuity frameworks.
- Develops, conducts, and documents regular IT risk assessments and treatment plans with recommendations, business performances and expected costs/benefits.
- Develops, conducts, and documents regular business impact analysis and IT continuity plans.
- Maintains an up-to-date understanding of industry best practices, changes in business requirements, and changes in legal or regulatory environments that could require changes to the District's established IT risk appetite, risk tolerance, continuity plan, policies or practices.
- Coordinates with Project Management Offices at various organizational levels to ensure IT risks are properly quantified, prioritized, documented, treated, monitored and incorporate them into the overall IT risk management program.
- Creates and maintains a centralized IT risk register and an IT continuity plan to manage all IT risks related information and document changes in business continuity requirements.
- 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 and IT continuity stakeholders on deficiencies identified in reviews, risk assessments, IT continuity tests, and IT audits to ensure that that effective and appropriate IT risk remediation and IT continuity 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, implements, conducts, and operates an IT risk and continuity plan training program for all concerned parties regarding their roles and responsibilities.
- 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, ISO 22301 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. Experience conducting business continuity reviews, assessments and developing continuity plans is preferable. Supervisory experience is also preferred.

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), Certified Business Continuity Professional (CBCP) or equivalent certification is preferred.

A valid driver's license to legally operate a motor vehicle in the State of California and the use of a motor vehicle, or the ability to utilize an alternative method of transportation.

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.

Revised
04-09-20
JAP

Updated
06-13-25
Transportation
Language Only