Internal Controls, Security & Risk Management - Information Security and Risk

Job Family	Grade 14 - Individual Contributor	Grade 15 - Management Track
Information Security and Risk	Information Security and Risk Manager	Information Security and Risk Director
Purpose:	Conducts Information Security assessments of diverse IT projects that include but are not exclusive to: Information Systems, Platforms, IT Infrastructure, and Processes to ensure compliance with established Columbia University and applicable regulatory requirements.	Overall responsibility to review IT security control and process requirements for existing and new IT systems and ensure that they are in compliance with Columbia University IT policies, procedures and standards.
Relation to Supervision:	Works independently while leading and coordinating all levels of activities including project lifecycle and day to day operations.	Reports to senior leadership team member. Sets direction and goals for department and/or team.
Architecture, Design, Development and Installation:	Advises on University initiatives and IT projects, provide evaluation of IT proposals to ensure that adequate controls are established.	Assess existing and new technology in the University IT environment landscape to determine overall risk to the University environment. Communicates with senior management on system-wide issues recommending solutions including resources needed, time required and benefits to be achieved.
Relationship Management:	Collaborate with various technical and functional support teams and provide security consultation.	Responsible for inclusion of security controls in system developments, participation in information security initiatives and ongoing compliance aspects of Information Security at CUIT, providing leadership, strategic, and line management directions.
Education & Experience:	Bachelor's degree and/or its equivalent required. Minimum 5-7 years related experience. Expert level networking knowledge and experience with a specific technical specialty.	Bachelor's degree and/or its equivalent required. Minimum 7-9 years related experience. Experience in all relevant technical specialties, methodologies and tools. Prior managerial experience required.
Soft skills:	Demonstrates excellence in a variety of competencies including teamwork/collaboration, analytical thinking, communication, influencing skills, and proven ability to act as a change agent.	Demonstrates excellence in a variety of competencies including ability to lead a team, teamwork/collaboration with technical and functional clients/peers, analytical thinking, communication and influencing skills. High degree of emotional intelligence. Proven ability to act as a change agent.

Technical Skills:	Working knowledge and/or technical experiences in multiple technologies: Databases, Windows,Unix/Linux, Network Protocols, Analytic Tools, Firewalls, Routers/Switches, Web Technology. Preferred: Accreditation in CISA (Certified Information Systems Auditor), CISM (Certified Information Security Manager), CRISC (Certified in Risk and Information Systems Control), or CISSP (Certified Information Systems Security Professional).	Broad functional and/or technical experience in all relevant applications design and development languages, methodologies and tools such as multiple platforms (e.g., Client Server, Database, Web technology, Network, Telecommunications, ERM Systems, etc.). Preferred: Accreditation in CISA (Certified Information Systems Auditor), CISM (Certified Information Security Manager), CRISC (Certified in Risk and Information Systems Control), or CISSP (Certified Information Systems Security Professional).