Dariia Kukshyn

JOBS

1. Senior Director, Information Security Risk Management – https://www.indeed.com/viewjob?jk=f2d6d87c331d09ca&tk=1emhaaaqvt4oq800&from=serp&vjs=3
2. Manager, Information Security Risk Management – https://www.indeed.com/viewjob?jk=bf309525b20287c7&tk=1emhdm16rsa0u800&from=serp&vjs=3
3. IT Risk Manager – https://www.indeed.com/viewjob?jk=35b3a586dc8c73d9&from=serp&from=mobRdr&utm_source=%2Fm%2F&utm_medium=redir&utm_campaign=dt

INFORMATION RISK MANAGER POSITION REQUIREMENTS

1. Job Description

The Information Security Risk Management plays a critical role in supporting the Information Security program achieve its objectives in key areas such as; information security and third party risk management, information security policy governance, operational risk reporting and analytics, and security and privacy awareness and training.

The Risk Manager is responsible for identifying, analyzing, tracking, and reporting on risks to information assets. This position has global responsibility for developing and executing components of the Risk Management Program including third-party and supply chain risk management, customer compliance, data protection, and policy exception. The Manager will update and maintain appropriate risk management processes to identify and treat risk.

The person leads the review of assessment findings, documentation, technology processes, and implementing controls in a wide range of environments.

The person manages the development and ongoing collection and reporting of information security metrics across functional leaders including identification, standardization, issue spotting, and presentation.

Responsibilities:

- Develop, implement, monitor and report on all aspects of an enhanced and robust Third-Party Risk Management, Provider Risk Management, and Project Risk Assessment capability.
- Maintain and update information security risk management framework, program guidelines, and Standard Operating Procedures (SOPs). Participate in the development and maintenance of supporting operating procedures.
- Review, update, and track action plans for identified risks and treatment plans within the established governance process involving business, audit, legal, and IT stakeholders.

- Lead the independent risk assessment of the provider, partners, suppliers, technology, security and resilience programs and provide effective challenge to the design and execution of technical and procedural controls.
- Conduct assessments with business partners to understand data protection challenges and opportunities for program improvements.
- Identify potential areas of compliance vulnerability and risk; develops/implements corrective action plans for resolution of problematic issues and provides general guidance on how to avoid or deal with similar situations in the future.
- Lead enterprise information strategies, planning, and priorities to expand our existing strategic risk management capabilities into the next level of tactical risks in cyber and business continuity, allowing us to identify and manage more discrete risks.
- Lead the security and privacy awareness and training program and present measurable progress.

2. Required Education

- Bachelor's Degree in Information Technology, Information Systems Security, Cybersecurity, or related field

3. Required Skills + Working Experience

- Industry knowledge of information assurance (IA) principles and organizational requirements that are relevant to confidentiality, integrity, and availability of data.
- Understanding of Security and Infrastructure Architecture/Technologies: including but not limited to Routers, Firewalls, IDS, PKI, VPN, Two Factor Authentication, Identity Management, Data Leak Prevention, Encryption, Application Security, Vulnerability Scanners, Penetration Testing, Windows and Unix Systems Security, Security Information Management and Event Correlation.
- Maintains knowledge of risks related to the information assets and intellectual property utilized by a global research, instrumentation, higher education, and gemstone grading business.
- Experience with demand, resource, and project management methods and working with a portfolio of security related projects.
- 2+ years of experience managing people and program for large enterprises.
- Minimum 5 years' experience in a related Information Security, Audit, or IT function.
- Demonstrated understanding of IT and Information Security frameworks (e.g., NIST CSF, ISO 27001, COBIT).

4. Personal Qualities

- Exceptional communication skills, both verbal and written. Excellent analytical and problem solving skills. Must be able to pay close attention to detail and understand written and oral instructions.
- Proven leadership skills demonstrating strong judgment.

- Demonstrates cooperation, flexibility, reliability, and dependability in all daily work activities and a willingness to collaborate with others.
- In addition, requires business acumen, strategic thinking, financial analytical skills and decision-making skills.

5. Certification

- CISSP (Certified Information Systems Security Professional) desirable.
- CISM/CISA (Certified Information Security Manager/Auditor) desirable.
- SANS GIAC (Global Information Assurance Certification) desirable.