Title

IT Security Manager – Security Risk Assessment Manager

Description

This position reports to the Chief Information Security Officer and is responsible for designing, implementing, managing, and overseeing the Information Security Risk Assessment process and procedures to ensure The company compliance with related regulations and industry requirements (i.e., HIPAA, Meaningful Use, FISMA, PCI, etc.). The manager is expected to be fully aware of the enterprise's security goals as established by its stated policies, procedures and guidelines and to actively work towards upholding those goals.

Responsibilities

- Manage a team and perform information security risk assessments of existing and new technology solutions as well as third parties. Oversee and track the remediation plans for all identified risks.
- Advise and assist project teams regarding compensating control alternatives where security requirements cannot be met.
- Provide technical and best practice guidance to remediate IT risks taking into account specific complexities of each business unit.
- Provide expert and complex level advisories on IT Risk framework, policies, standards and guidelines and contribute to their development where appropriate.
- Develop and maintain key relationships with core teams in order to provide advice and oversight on new initiatives.
- Contribute to quarterly reports to MCIT Business-Partners on their respective application, infrastructure, and third party risk postures.
- Review security and control processes along with associated documentation and reporting.
- Review key audit and regulatory findings and develop and communicate risk themes and solutions to them.
- Promote a risk aware culture and communicate best practices to business and IT contacts.
- Leverage information on current threats to focus business and IT attention on emerging risk themes and issues.
- Lead and direct a small team in the security assessment process. Set clear goals and expectations that accomplish objectives.
- Mentor and develop staff members and create a positive work environment that supports engagement with others.

Position Requirements

Formal Education & Certification

- Bachelor's degree from an accredited college/university; Master's degree from an accredited college/university preferred

- CISSP – Certified Information Systems Security Professional (ISC2)
- CISA – Certified Information System Auditor

Knowledge & Experience

- Minimum six years of progressive experience in leading security and compliance management programs; interactions with and support of clients; risk management and other GRC responsibilities within a large IT organization, preferably within a professional services firm or similar.
- Demonstrated experience with managing information security functions, including governance, frameworks, processes, tools, scorecards, and dashboards under aggressive deadlines and with competing priorities.
- Knowledge of industry regulations and standards (e.g. HIPAA, Meaningful Use, FISMA, PCI) as well as core technology infrastructure (e.g. firewalls, vpns, servers, databases, Internet technologies).
- Proven experience interacting with regulators, internal auditors and/or external auditors.
- Demonstrated knowledge of industry authoritative sources such as COBIT, NIST, and ISO standards
- Working knowledge of GRC tools such as Symantec CCS, Archer GRC, Modulo Risk Manager.
- Certification requirements: CISSP, CISM, CISA, ISO 27001 Auditor, LSS Green Belt, CRISC, CIPP, CGEIT or ITIL

Personal Attributes

- Ability to effectively prioritize and execute multiple assignments and tasks in a high-pressure environment.
- Good written, oral, and interpersonal communication skills.
- Ability to conduct research into IT security issues and products as required.
- Ability to present ideas in business-friendly and user-friendly language.
- Highly self-motivated and shows initiative. Ability to work independently and with other teams when needed to troubleshoot problems.
- Capacity to learn new software and become proficient to provide support.
- Keen attention to detail.
- Team-oriented and skilled in working within a collaborative environment.

Work Conditions

- On-site work week with on-call availability.

Questions and resume submission may be forwarded to Nadia Brika
NBrika@execu-search.com