



The position is responsible for Security Operations in the LFTS business. The primary responsibilities include: Vulnerability Management, Incident Management, Execution of Security Standards, Defining Application Security Standards and Security Monitoring.

This position acts as liaison to the Security and Compliance Department and well as an ongoing solid working relationship with internal customers at the Director and VP level.

#### Responsibilities:

- Implement the organization's information security policies and procedures.
- Monitor compliance with the organization's information security policies and procedures among employees, contractors, alliances, and other third parties, and champion continuous improvement as well as remediation efforts with appropriate department managers or administrators.
- Monitor internal control systems to ensure that appropriate information access levels and security clearances are maintained.
- Perform information security risk assessments and serves as the internal information security auditor.
- Serve as an internal information security consultant to the organization, monitors advancements in information security technologies.
- Initiate, facilitate, and promote activities to foster information security awareness within the organization.
- Monitor changes in legislation and accreditation standards that affect information security.
- Act as liaison to the Information Systems Department.
- Lead and coordinate the activities of the Security Operations function, as well as planning and communicating resource requirements, and ensure successful and timely completion of projects and ISMS or ITGC remediation efforts.
- Design and execute security operations processes, identify and measure critical security operations metrics, and continually improve the efficiency and effectiveness of the Security Operations function.
- Work closely with peer managers to identify and implement process changes, improvements and efficiencies, and ensure solid security practices.
- Responsible for aligning the security functions with the organization's overall business objectives.
- Identify and respond to security incidents, including investigation, response, and resolution.
- Assist Senior Management in defining the overall information security strategy.
- Provide security advice and guidance to architecture, operations and management.
- Collaborate with development to mitigate risks and enhance application security.
- Implement cost effective security controls to meet corporate security requirements.
- Possible interaction with external clients during the sales process to describe security measures employed.

#### Skill/Experience/Education Requirements:

- 5-10 years progressive experience in IT security roles
- Bachelor's Degree (preferably in information management systems) or equivalent professional experience.
- CISSP, SSCP, CISM, or CISA certification
- Understanding of ISO 27001 framework
- Strong interpersonal and communication skills to work effectively with IT and business units.
- Demonstrated ability to translate between business and security requirements for technical and non-technical managers.
- Experience as mentor or trainer within a technical field.

#### Well-qualified candidates will have:

- Experience with ISO-27001, SAS-70/II, PCI, and/or HIPAA compliance projects
- Experience securing custom-developed products in a hosted/SaaS environment