Position:
To ensure data protection, regulatory and Sarbanes-Oxley compliance with all information systems. Responsibility for enterprise information security standards.

Responsibilities:

- Develops and implements information security standards and procedures
- Ensures that Sarbanes-Oxley requirements are fully met across the global Applications portfolio
- Ensures that all information systems are functional and secure
- Provides guidance to Infrastructure and Application Delivery groups regarding best practices relating to cloud, mobile, desktop and server-level security
- Reviews and provides improvement recommendations for global Change Control processes, including quality assurance of all change controls
- Functions as point-of-contact representing IT in all internal and external audit matters
- Assists with the management and visibility of global application audit issues.
- Conducts studies within and outside the organization to ensure compliance with standards and currency with industry security norms
- Assists in the development, maintenance, and implementation of application control policies, procedures, and standards
- Periodically review existing standards and procedures relating to security framework (IT general controls, COBIT, COSO) and update as necessary
- Responsible for implementing testing methods and procedures to detect security vulnerabilities
- Responsible for ensuring that tools or technologies are implemented to reduce the risk of system attacks.
- Monitors compliance metrics to ensure accurate reporting and continuous improvement
- Provides status reporting of all compliance metrics; coordinates quarterly metric reporting for the IT management team, CIO, and other executive leaders as necessary
- Provides monthly IT security updates to educate the Leadership team on latest trends in technology.

Technical Requirements:

- Extensive background in best-practice security practices, both technological and physical
- Extensive knowledge of information security frameworks (COBIT)
- Knowledge of encryption technology, best practices, and implementation
- Experience in PCI credit card processing as well as eCommerce Cyber security
- Broad-based knowledge of IT operating systems (Windows, UNIX), platforms (mainframe, AS400), mobility technology (Apple iOS and Blackberry devices)
- Understanding of global business regulations, country-specific privacy laws, and how they impact a global company
- Demonstrates strong organizational; project management; analytical, problem-solving and communication skills
- Evaluates alternatives to mitigate application risks and communicates potential solutions to management
- Working knowledge in multiple architecture domains (technology, data etc.).

Analytical Skills:

- Excellent written and verbal English communication skills
- Strong inter-personal skills
- Candidates must have the ability to manage multiple priorities concurrently
- Strong analytical approach to problem solving and solution development
- Experience working with a very formal change control process
- Willingness to adhere to a standard global process model
- Ability to effectively work in a global team
- Self-starter with the ability to independently resolve issues and deliver results
- Experience developing and monitoring continuous improvement application metrics is highly preferred

Education:

- Bachelor's Degree in Computer Science, Information Systems, related filed or equivalent work experience
- Master's Degree in Computer Science, Information Systems, or other related field is preferred
- One or more certificates (CISA, CISSP, etc.) preferred

Other Requirements:

- Minimum 8 years of IT security management work experience, some of which was in a large, global environment
- Prior experience in a senior management position is required, preferably in an industry with extensive security requirements such as the financial, retail, insurance or defense industry.
- Ability to travel internationally – up to 25%