

IT Security Risk Analyst (Sr. Engineer)

## Description

The successful candidate will work with application, database and/or infrastructure IT project teams to plan and conduct risk assessment activities on Client IT resources to prevent or remediate significant risks. He/she will identify and document vulnerabilities and threats using repeatable risk assessment methodologies and processes. This may include producing and analyzing output from infrastructure, database, or web application vulnerability assessments and developing spreadsheets, diagrams, and Word documents as requested.

He/she will also identify and document IT security requirements required to remediate significant risks and achieve desired levels of confidentiality, integrity, and availability based on internal policies and industry best practices. He/she will then advise, as needed, the resource owner who decides what actions to take regarding mitigation strategies and the implementation of security controls.

The successful candidate will enable business goals by reviewing change management requests for adherence to IT security requirements, policies, and technical standards in a timely manner. He/she will also review proposed appliance, product, and network security designs for adequate IT security consideration, and collaborate to produce an "As-Is" view of security architecture as well as a "To-Be" security architecture.

He/she needs to be able to effectively communicate with management, engineers, customers and others to help them learn their roles and responsibilities in the implementation and maintenance of appropriate security controls. He/she needs to have an appreciation for the need to balance controls that are applied against potential impacts on business functionality and performance.

The successful candidate will have a demeanor of maturity and professionalism that promotes trust and respect for the entire risk management team in those with whom the team interacts.

He/she will be able to communicate with others (written and verbal) in a way that shows proper respect for their position and for them as individuals. He/she will be able to be trusted to work in sensitive situations and with sensitive information and keep confidences.

## Qualifications

- Bachelor's Degree or equivalent work experience
- 8-10 years experience in a core IT technology (e.g. software developer, network engineer, database engineer) where management of risk was part of the work experience
- Broad background in IT technologies, processes, standards, and best practices
- Demonstrated small, self-directed team player; a self-starter who does not require close supervision
- Demonstrated ability to conceptualize, analyze, and communicate complex issues and concerns to technical and non-technical management and workers
- Demonstrated ability to develop, refine, and follow processes

- Familiarity with security standards and best practices such as those specified by the National Institute of Standards and Technology, Payment Card Industry, ISO 27000, Center for Internet Security, SANS Institute, or COBIT required.
- IT Security certification (CISSP, CCSP, SSCP, GSEC, GISF, etc.) required. Other technical certifications (MCSE, CCNP, CCNA, CCIE, etc.) a plus.

<http://www.slc-staffing.com>