IT Risk Analyst Job Description

Duties and Responsibilities:

- Correlates threat data from various sources to complete a comprehensive picture of potential cyber-attacks and decipher attack motivations and techniques
- Works closely with other technical, incident management, and forensic personnel to develop a fuller understanding of the intent, objectives, and activities of cyber threat actors and enables a world-class cyber defense program
- Responsible for conducting research and evaluating technical and all-source cyber intelligence to develop in-depth assessments of threats to the organization's networks, systems, users, and data
- Serves as liaison and point of contact for new issues and vetting
- Conducts complex cyber intelligence analysis and awareness through collaboration with other internal experts and trusted outside organizations
- Performs threat analysis utilizing a combination of standard intelligence methods and business processes to uncover advanced threat actors
- Designs an innovative threat and security incident management solution
- Creates technical assessments and cyber threat profiles of current events on the basis of inventive collection and research using classified and open information sources to enables advanced threat intelligence
- Develops and maintains analytical procedures to meet changing requirements and enable more strategic detections
- Utilizes threat messaging, models, analyses, presentations, or recommendations to convey complicated technical or behavioral analysis to senior management
- Participates in a coverage model to prevent and remediate security threats against the organization
- Stays abreast of innovative business and technology trends in IT security, risk, and controls

- Advices leadership on technology initiatives that support latest trends in IT security, risk and controls
- Ensures effective execution of the risk management framework by managing relationships with key stakeholders within strategic business groups and technology
- Responsible for conducting deep dives on IT security-related processes and systems
- Verifies that IT risks are appropriately mitigated and leads multiple stakeholders in agreement on appropriate solutions/controls
- Responsible for identifying applicable regulatory risks from changes or additions to regulatory guidance and requirements
- Provides expertise for resolution and risk mitigation.
- Develops, tracks, and reports on Key Risk Indicators (KRIs) for information technology
- Monitors, tracks, and reports mitigation and resolution of IT risks
- Performs process-level walkthroughs, control testing, etc. for the identification and assessment of IT risks and controls
- Effectively communicate key risks, findings, and recommendations for improvement with key stakeholders.

IT Risk Analyst Requirements – Skills, Knowledge, and Abilities

- Education: To become an IT risk analyst requires a minimum of Bachelor's degree in Computer Science, Cyber Security, Information Technology, or a similar technical degree
- Certification: Analysts may be required to be Certified Information Systems Security Professional (CISSP), Certified Information Security Manager, (CISM), Certified Information Systems Auditor (CISA), or Certified in Risk and Information Systems Control (CRISC), depending on the preference of the organization
- Knowledge: They require an understanding of key technology concepts such as access control, confidential data, encryption, business continuity, info-sec scans, and vendor apps. They also require strong knowledge of IT organization business processes and systems including (IT Security, data management, architectural and planning, technology life cycle management, regulatory concerns). They may also be required to

possess solid understanding of risk management functions, including IT audit, cyber security, and/or IT compliance. Experience or knowledge of 3rd party/vendor management lifecycle may also be required

- Communication skills: They require strong oral and written communication skills to work effectively with employees at all levels of the organization. It is also essential that they are comfortable driving conversations with teams with varied backgrounds and purpose, such as conversing with Risk Team/Info-Sec/Technology Teams/Vendors/ Vendor Managers, etc. It is also important that they can be receptive to guidance from manager and able to effectively communicate results to manager
- Organizational skills: IT risk analysts must be highly organized with ability to prioritize and multi-task, as well as able to thrive in a fast paced environment
- Excellent leadership skills: They require this skill to influence other employees and ensure compliance with security controls.
- Computer skills: They require advanced computer skills and must be proficient with Microsoft Excel, Word, and PowerPoint
- They require excellent problem solving skills and the ability to be highly productive, both working alone and as part of a team.