Downloaded from <https://www.velvetjobs.com/job-descriptions/information-security-risk>

# Example of Information Security Risk Job Description

Our innovative and growing company is looking to fill the role of information security risk. To join our growing team, please review the list of responsibilities and qualifications.

## Responsibilities for information security risk

* Institute a robust security awareness program
* Maintain the Disaster Recovery Program to ensure systems are appropriately protected and testing, training and exercises take place
* Develop IT Risk Management program inclusive of education, procedures, risk register maintenance, action plans and management reporting to ensure projects and activities are being performed in accordance with company’s risk appetite
* Maintain and enhance the Vulnerability Management Program to provide appropriate protections for various system types including business tools, lab equipment and manufacturing systems
* Lead internal Information Security audit and assessment activities and coordinate remediation efforts
* Member of the Information Technology leadership team, providing technical knowledge and managerial expertise, assisting with the development of specific goal for the optimum use and management of IT resources
* Proactively research and stay up to date on latest access security issues
* Form and maintain relationships globally to understand changes within countries, markets and globally
* Manage oversight of control and process owners globally to ensure requirements are met and security policies are adhered to
* External email monitoring via Vontu to identify any unauthorized information sent externally

## Qualifications for information security risk

* Must be able to see the customer perspective, from a business point of view, the most secure solution is not always workable or realistic considering costs and benefits
* Network or system administration experience
* 10 or more years of technology experience, either in technology infrastructure or application development
* Strong application or infrastructure information security knowledge including but not limited to secure coding practices, secure infrastructure configuration & design, security vulnerabilities
* Strong understanding of the regulatory requirements around business continuity and/or technology control across the Asia markets is a significant plus
* Business continuity knowledge in developing or maintaining business continuity plans, technology resiliency (disaster recovery), business recovery sites development and testing, and technology crisis management a plus