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

# Example of Senior Information Security Advisor Job Description

Our company is looking for a senior information security advisor. We appreciate you taking the time to review the list of qualifications and to apply for the position. If you don’t fill all of the qualifications, you may still be considered depending on your level of experience.

## Responsibilities for senior information security advisor

* Work hand-in-hand with other Security Advisors and all relevant stakeholders to identify, remediate and bring closure to all potential security related threats
* Document incident response SOPs and playbooks
* Event monitoring process and technical improvements
* Participate in Internal/External Compliance Audits
* Produce Weekly/Monthly/Yearly Incident Response KPI/KRI metrics
* Potential involvement in Red Team campaigns
* Identify gaps and recommend improvements to enterprise technology environment across all platforms, with a goal to enhance the overall security posture of Cigna
* Consult broadly with the Business Groups and Enterprise Services using technical expertise to guide and influence implementation of security in wide or high-impact technology decisions and initiatives
* Provide the management team with an in-depth analysis of information security trends, the status of identified risks, penetration testing and vulnerability scan results, security incidents, current work activities, and work completed by the department
* Provide support on IT security events and work with IT and business organization within the Incident Management processes for those events by gathering information for analysis from various internal and external sources

## Qualifications for senior information security advisor

* Requires BS/BA in related field
* Must have a Bachelor’s degree in Information Security, Information Technology, Information Systems Management, Computer Science, Engineering or related field(s) or equivalent demonstrated work experience
* Minimum of 5 years of directly related experience in Information Technology
* Bachelor’s Degree in Information Security, Information Technology, Information Systems Management, Computer Science, or Engineering
* Experience with defense in depth, trust levels, privileges and Permissions experience in application penetration testing
* Professional information security certifications, such as a Certified Information Systems Security Professional (CISSP) or other similar credentials