| Job Description | |
|---|---|
| Position Name | Security Test Manager |
| Designation | Security Test Manager |
| Department | MAP_IT |
| Place of Work | BHOPAL |
| Job Type | Contractual ( Upto 2 years ) extendable basis performance |

**Job Objective**

IT Security manager will oversee a team of auditors and ensure their compliance with corporate and government standards especially as per the CERT-IN norms.

The IT Security manager shall assign staff, supervise planning and oversee specific audits as well as reviews all work papers, ensuring audits are performed with best industry practices and within the time & budget allotted.

The IT Security audit manager shall point out system flaws and promote efficient practices by recommending improvements in processing capability, user interface, and security designs.

**Primary Responsibilities Of The Role**

**Job Role Pointers**

1. IT Security manager will oversee a team of auditors and ensure their compliance with corporate and government standards especially as per the CERT-IN norms.
2. The IT Security manager shall assign staff, supervise planning and oversee specific audits as well as reviews all work papers, ensuring audits are performed with best industry practices and within the time & budget allotted.
3. The IT Security audit manager shall point out system flaws and promote efficient practices by recommending improvements in processing capability, user interface, and security designs.
4. The Security Manager shall review and finalize the audit plans, test cases, and test scenarios to perform the security audit.
5. The Security Manager will overall responsible for VAPT (Vulnerability Assessment & Penetration Testing) and finalization of audit reports, co-ordination with CERT-IN for filing the quarterly/yearly reports.

**Candidate Profile Details**

| Essential Criteria | Desirable Skills & Experience |
|---|---|

**Education Details**

**Graduation Details –**

- B.E / B.Tech (in any stream)/ BSc (CS/IT) / MCA / MSc (CS/IT) / BCA or post-graduation in (CS/IT)

**Certification Details**

- Certified Information Systems Security Professional (CISSP)
- Certified Information Security Manager (CISM) of ISACA
- Certified Information Systems Auditor (CISA) of ISACA
- Diploma in Information Systems Audit (ISA or DISA) of ICAI
- Certified Ethical Hacker (CEH) by EC-Council
- Any other formal IT Security related qualification like Offensive Security, GSSP, CSSLP, ECSP, CCIE-Security, JNCIE-Security, ISMS LA , GIAC , CompTIA Security+ Industry prevelant GRC certifications etc.

**Work Experience**

- 10+ years' of relevant experience in IT Network and Infrastructure security implementation and operations in which 2 year should be at managerial role.

**Preferable**

- Should have overseen at least eight IT Security Audits, preferably five of which should be in the last 12 months in line with the CERT-IN norms.
- 5 years of relevant experience in security operations setup as an Information Security / Infrastructure Security / Application Security / Network Security / Cyber Security Engineer/ Consultant / manager.
- Exposure to security standards like ISO 27001, PCI-DSS etc.
- Exposure to cyber security frameworks like OWASP, SANS, NIST etc.
- Should have experience with IT security operations (SOC) and NOC (Network Operations).
- Should have experience IT infrastructure & Web Application security.
- Experience and knowledge of Web Application Security, mobile application security OWASP/SANS etc.
- Should have experience in Vulnerability identification, management and prioritization.
- Experience in analysing and in identifying the vulnerabilities manually.
- Experience in application and network penetration testing.
- Experience in Vulnerability scanning - Network and Application scans, Vulnerability Assessment, Management & Security Auditing.
- Experience in using tools such as Nessus, Acunetix , Appscan etc.
- Experience in using Burp suite, Scripts and Kali Linux, Metaexploit and other such static analysis tools.
- Experience in developing the hardening guidelines with inputs on improving and maintaining baseline standards.
- Should have the ability to stay organized, and possess excellent communication skills.
- Vulnerability & Risk assessment and management.
- Network and Infrastructure Security assessment and management.
- Server, Desktop and Endpoint Security planning, implementation and hardening.
- Security Incident management. Exposure to SIEM.