

Job Description

POSITION DETAILS			
Position Title/Functional Designation	AVP_ Information Security Assessment	Company	Poonawalla Fincorp Limited
Division / Department	Risk – Information Security		
Principal Accountabilities			
<p>Experience:</p> <ul style="list-style-type: none">• 10 years+ in Application security testing with a proven ability to engage with Senior Management and various business team.• 5+ years’ experience in implementing Information security controls in an organization.• 3+ years of experience in Cloud Based Information Security Key Responsibilities at Poonawalla Fincorp, the person would need to work closely with the Technology and Governance teams to identify risks from internal and external environment and design, deploy and maintain adequate controls to reduce risks. <p>Application Security testing -</p> <ul style="list-style-type: none">• Well versed with OWASP – Top Ten and WASC Threat Classifications• Expertise in Vulnerability Assessment and Penetration Testing of Web Applications and Source Code Reviews• Well versed in OWASP Code Review concepts & identifiers• Familiar with popular tools: * Application Proxy: Burp suite, Paros, OWASP ZAP, WireShark *• Application Security Testing/Penetration Testing (Web-based, Thick client, web services, Mobile)• Network Security Testing/Penetration Testing (Network, OS, Databases etc)• Static Code Analysis/ Secure Code Review. <p>Application security architecture review-</p> <ul style="list-style-type: none">• Collaborate with business and IT team to perform detail application architecture review.• Threat modelling and present to respective team to ensure mitigation of reported risk/threats. <p>Implement and govern cloud security testing -</p> <ul style="list-style-type: none">• To assess the security posture of cloud infrastructure, platforms, and services (IaaS, PaaS, SaaS).• Evaluate cloud configuration settings for adherence to security best practices.• Identify potential misconfigurations, access control issues, and data leakage risks.• Cloud Security – AWS and Azure, GCP, Oracle domain. (Any one to two cloud domains he/she should have knowledge.)• Cloud Application Pentest / Cloud Network Pentest• Cloud Security Architecture Review for Infrastructure and Application• Cloud Security Configuration Review• <p>Assurance</p> <ul style="list-style-type: none">• Perform various assessment exercises to identify PFL system and technology vulnerabilities and threats to address loopholes based on industry/global cyber threats viz. red team, ransomware readiness, config review but not limited. And ensure its remediation as per Information Security and Cybersecurity Policy, Common Security Standards, Technical Security Standards and CISO Directives.			

Job Description

Qualification, Experience & Skills

- Bachelor's degree in engineering or Graduation in Computer Science degree
- 10-15 years' experience in Privacy, Information Security, Compliance, Risk and Regulatory is mandatory for this role. Experience in BFSI / NBFC Domain will be preferred.
- Any one Information security credentials CISSP, CISM, CISA, PCI DSS, ISMS Lead Auditor, Compliance, Risk Assessment, ISO 27001, Business Continuity Management. (or equivalent) is an advantage.
- Excellent communication skills in verbal and writing. Problem solving attitude and willingness to learn
- Age Criteria – 30 to 45 Years