



Job Descriptions: IT Security

Summary -

The Security Manager shall be responsible for managing and strengthening the Bank's overall information security, cyber security, physical security coordination, regulatory compliance, and risk management framework in line with guidelines issued by the Reserve Bank of India, applicable banking regulations, and internal policies.

The role includes implementation of security controls, monitoring cyber risks, incident management, vendor security governance, awareness programs, and ensuring protection of Bank data, systems, applications, networks, and digital banking channels.

Key Responsibilities:

A. Information & Cyber Security Management:

- Implement and monitor the Bank's Information Security Management Framework
- Ensure compliance with RBI cyber security and IT governance guidelines
- Monitor security operations, alerts, vulnerabilities, and cyber threats
- Coordinate implementation of:
 - Firewall security
 - Endpoint security
 - Data Loss Prevention (DLP)
 - SIEM/SOC monitoring
 - Multi-factor authentication
 - Privileged access management
 - Network security controls
- Conduct periodic vulnerability assessments and penetration testing (VAPT)
- Ensure secure configuration and hardening of systems and applications
- Monitor patch management and security updates

B. Regulatory & Compliance Responsibilities:

- Ensure compliance with:
 - RBI IT Governance Directions
 - RBI Cyber Security Framework
 - DPDP Act, 2023
 - NPCI security requirements
 - CERT-In advisories
 - Audit and compliance observations
- Support internal, statutory, RBI, IS audit, and cyber security audits
- Maintain required security documentation, policies, SOPs, and compliance reports
- Coordinate closure of audit observations within timelines

C. Security Monitoring & Incident Response:

- Monitor cyber security incidents and coordinate incident response activities
- Investigate security breaches, phishing attempts, malware infections, and fraud-related cyber events

- Coordinate with CERT-In, law enforcement, and regulatory agencies where required
- Maintain incident registers and Root Cause Analysis (RCA) reports
- Support cyber crisis management and disaster recovery activities

D. Risk Management:

- Identify and assess IT and cyber security risks
- Maintain risk register and mitigation plans
- Conduct vendor / third-party security risk assessments
- Review cloud security and outsourced IT environments
- Ensure risk-based security controls are implemented

E. User Access & Identity Management:

- Monitor user access management controls
- Ensure maker-checker implementation
- Review privileged and admin access periodically
- Ensure role-based access control (RBAC) implementation
- Coordinate periodic access recertification exercises

F. Data Protection & Privacy:

- Ensure protection of customer and Bank data
- Monitor implementation of:
 - Data classification
 - Data retention
 - Encryption
 - Secure disposal
 - Backup security
- Support implementation of privacy and consent management requirements under the DPDP framework

G. Security Awareness & Training:

- Conduct cyber security awareness programs for employees
- Organize phishing simulation exercises
- Conduct training for branch staff and IT users
- Promote security best practices across the Bank

H. Coordination & Governance:

- Coordinate with:
 - IT team
 - Core Banking vendor
 - SOC/SIEM providers
 - Auditors
 - Regulatory authorities
 - Branch operations
- Present security status and risk reports to senior management and committees

- Support Information Security Committee meetings

Educational Qualification:

- Bachelor's Degree in:
 - Computer Science
 - Information Technology
 - Cyber Security
 - Electronics
 - Engineering
- Preferred:
 - Master's Degree / MBA (IT)
- Security certifications such as:
 - CISM
 - CEH
 - ISO 27001 LA/LI
 - CompTIA Security+
 - CCNA Security

Experience:

- Minimum 5–10 years of experience in:
 - Information Security
 - Cyber Security
 - Banking IT Security
 - Risk & Compliance
- Experience in Banking / NBFC / Cooperative Banking preferred
- Experience handling RBI audits and cyber security compliance preferred

Required Skills:

- Knowledge of banking cyber security frameworks
- Understanding of RBI regulatory requirements
- Incident response and risk assessment skills
- Knowledge of:
 - Firewalls
 - SIEM
 - Endpoint security
 - IAM
 - VAPT
 - Network security
- Documentation and policy drafting skills
- Analytical and problem-solving skills
- Team coordination and communication abilities

Skills and competencies

Candidate should preferably have:

- Understanding of Core Banking Systems (CBS)
- Experience in UCB / Cooperative Bank operations
- Knowledge of NPCI ecosystem:
 - UPI
 - IMPS
 - AEPS
 - ATM switching
- Exposure to outsourcing and Fin Tech risk management