Position/Title: Risk Manager – Information Security

Job Role

As Manager – Information Security, you will be responsible for establishing and enforcing security protocols that safeguard Company's information systems, digital assets, and customer data.

Key Responsibilities

1. **Develop & Implement Information Security Strategy** – Design and execute a comprehensive information security roadmap aligned with company's digital infrastructure, business model, and regulatory obligations.
2. **Cybersecurity Risk Management** – Identify, assess, and mitigate cybersecurity risks across infrastructure, applications, APIs, mobile platforms, and third-party integrations.
3. **Regulatory Compliance & SBP Alignment** – Ensure full compliance with SBP guidelines and international security frameworks (e.g., ISO 27001, NIST), and act as the point of contact for regulator-driven security reviews.
4. **Security Architecture & Operations** – Oversee the design, configuration, and monitoring of security systems including firewalls, endpoint protection, SIEM, encryption, and identity/access management tools.
5. **Incident Response & Threat Management** – Develop and lead the incident response process, including detection, containment, investigation, recovery, and post-mortem reporting.
6. **Security Audits & Penetration Testing** – Coordinate regular internal and third-party audits, vulnerability assessments, and penetration testing to ensure system hardening.
7. **Employee Awareness & Policy Enforcement** – Establish security awareness programs, train internal staff, and enforce information security policies across all departments.
8. **Collaboration with Internal Audit & IT** – Work closely with Internal Audit, Technology, and Compliance teams to ensure consistent enforcement of risk controls and secure infrastructure design.

Required Qualification: Masters/ Bachelor's degree (16 years of equivalent education) in Business Administration (Information Systems), Computer Science or related field from HEC recognized institution. Professional certifications such as **CISSP**, **CISM**, **CEH**, or **ISO 27001 Lead Implementer/Auditor** will be encouraged.

Experience: Minimum 03 years' post qualification experience in computer systems with specialization in information security will be highly preferred.

Age: Maximum 40 years (as of the last date of submission of application)

Job Location: Karachi

Relevant Expertise:

1. **Information Security Expertise** – Minimum 3 years of relevant experience in information security or cybersecurity roles, preferably within fintech, digital banking, or regulated financial institutions.
2. **Regulatory & Standards Knowledge** – Strong understanding of SBP cybersecurity guidelines, ISO 27001, NIST, and relevant global information security frameworks.
3. **Incident Management & Threat Response** – Demonstrated experience in handling security incidents, vulnerability assessments, and threat intelligence operations.
4. **Security Operations & Architecture** – Hands-on experience with firewalls, IDS/IPS, antivirus, endpoint protection, encryption, and secure network architecture.

Required Competencies:

1. **Technical Cybersecurity Proficiency** – Deep technical knowledge of cybersecurity tools, infrastructure protection, and digital risk management in consumer-facing platforms.
2. **Regulatory & Audit Readiness** – Proven track record of preparing for and managing regulator-led audits and aligning cybersecurity operations with legal and compliance standards.
3. **Risk & Policy Management** – Ability to define, implement, and enforce cybersecurity policies, standards, and control frameworks organization-wide.
4. **Cross-Functional Collaboration** – Strong interpersonal skills to work closely with technology, audit, risk, and compliance teams to embed a culture of security.
5. **Adaptability in Fast-Paced Environments** – Demonstrated ability to manage evolving security risks.