

Job Description for Chief Information Security Officer (CISO)

Location:	NABFINS Limited, Head Office, Bangalore
Years of experience:	5+ years
Desirable:	Prior experience in BFSI/Insurance sector is preferred

Chief Information Security Officer (CISO) is responsible for overseeing the overall information security strategy of the organization and is entrusted with the responsibility of developing, implementing and monitoring a strategic and comprehensive enterprise-wide information security and IT risk management.

Mandatory:

Minimum 5+ years of experience in IT/ Information Security, with at least 2 years in a senior leadership role (CISO / Deputy CISO / Head of Information Security).

Knowledge & Competence Areas:

- The candidate should demonstrate expertise and leadership-level understanding of IT Governance, Risk & Compliance:
- IT Act, Digital Personal Data Protection (DPDP) Act and associated rules thereunder, IRDAI and other Regulatory Guidelines, CERT-In cyber security circulars and RBI guidelines.

Regulatory and Compliance Responsibilities:

- Coordinate with regulatory and intelligence agencies including RBI, NABARD, IRDAI, and CERT-In CSITE for information sharing and compliance.
- Coordination with departments in NABFINS for the regulatory compliance.
- Ensure compliance with the IT Act, Digital Personal Data Protection (DPDP) Act, IRDAI Cybersecurity Guidelines, and other domestic and international standards.
- Liaise with the Company's Legal and Compliance teams to interpret regulatory updates and ensure timely security control alignment.
- Lead the development and maintenance of the organizational Data Governance framework, policies, and standards related to data classification, retention, and access controls.
- Oversee the resolution of audit observations and inspection findings from regulators, statutory auditors, and internal/external agencies.
- Coordination with the internal/external auditors aligned for IT audits such as Information Security audit, Vulnerability assessment and penetration test, Insurance Regulatory and Development Authority of India audit, RBI audit, and NABARD audit

Advisory and Reporting Responsibilities:

- Oversee the design and delivery of information security awareness and training programs for employees, vendors, and senior management, ensuring relevance, effectiveness, and compliance with regulatory requirements.
- Regularly brief top management, Risk Management Committee and the Board Risk/IT Committee on cyber security posture, risks, compliance, and initiatives.
- Preparation of agendas and presentation to the Board / IT committee.
- Oversee the development and ensure presentation of executive dashboards and key metrics on risk, compliance, incident management, and overall security posture to senior management, Board and ITSCB.

- Represent the Company in industry forums, regulatory committees, and technical conferences on information and cyber security.
- Advise leadership on emerging global threats, vulnerabilities, and recommended actions to strengthen the Company's resilience.
- Ensure transparent communication with stakeholders (internal and external) during cyber incidents as per crisis communication protocols.

Candidate must be well versed in:

- Cyber Risk Management
- Information Security Risk Management
- Third-Party Risk, Supply Chain Security
- Cyber Insurance
- Risk Quantification
- SIEM and SOC operations
- Incident detection and Response (EDR)
- Threat Intelligence
- Identity and Access Management (IAM)
- Privilege access management (PAM)
- Network Access Control (NAC)
- Zero Trust Architecture (ZTA)
- Cloud Application & Infrastructure Security
- Cloud Security
- Virtualization
- Secure Software Development Life Cycle (SDLC)
- Development, Security, and Operations (DevSecOps)
- API Security
- Data Protection & Resilience
- Data Security
- DLP (Data Loss Prevention)
- Security Testing
- DR & BCP
- Crisis Management
- Emerging Security Practices
- AI/ML in threat detection
- Security Automation
- Advanced Threat Hunting.

CISO – Roles and responsibilities

1. Review the information and Cyber security posture of the company
2. Identify the gaps in Cyber security and escalate the same to DIT
3. Present agendas on Cyber security related aspects to the Board/Committees of the Board
4. Conduct enterprise-wide cyber risk assessment for NABFINS across branches, HO, applications in use, etc.
5. Classification of risks identified and extending support to the Internal IT Team to ensure that the identified security control gaps are understood and duly remediated

6. Coordinating for conduct of Information Security Committee (ISC) meetings
7. Conduct cyber security awareness trainings to employees
8. Coordinating the conduct cyber resilience activities across the organization
9. Incident Management - Lead strategic response to information security incidents and provide post-event analyses
 - a. Preparation of detailed RCA
 - b. Drafting the response to queries raised by Regulators
10. Regular and adhoc reporting through regulatory portals
11. Coordinate the conduct of IS Audit, VAPT etc.
 - a. Devise Frameworks for IS Audits and VAPT
 - b. Coordinate with DIT for resolution of the issues identified during IS Audit/VAPT
 - c. Draft the compliance to VAPT, IS Audit observations
12. Annual review of all IT Policies for their adequacy and identify implementation gaps, if any
13. Ensure compliance to internal policies as well as Legal and Regulatory Guidelines (RBI, IRDAI) pertaining to IT
14. Define Key Risk Indicators (KRI) for monitoring cyber security resilience
15. Collaborate with CTO/CIO to create and implement enterprise-wide disaster recovery plans
16. Negotiate contracts with vendors and service providers for installing security products and services
17. Recognize the emerging technology trends and ensure cybersecurity controls are implemented to secure the ever-changing landscape
18. Explore latest tools for cyber resilience and inform the Management of their relevance, feasibility etc.
19. Revision of policies related to Information Technology (IT) and Information Security (IS) and presentation to Board and ITSCB.

Qualifications

1. Should be qualified with at least two of the following certifications
 - a. CISA (Certified Information Systems Auditor)
 - b. CISSP (Certified Information Systems Security Professional)
 - c. CISM (Certified Information Security Manager)
 - d. CEH (Certified Ethical Hacker)
2. Proven experience as a CISO or similar role in information security management and cybersecurity for at least 2 years

OR

- Experience in working on Information Security or Cyber Security domains for at least 5 years
3. Graduation – Preferably: Degree in Engineering, Computer Science/Information Technology or its equivalent.
 4. Experience and Knowledge of Security best practices across IT domains (Infrastructure, Application, Enterprise architecture etc.)
 5. Robust experience of designing and deploying security solutions
 6. Good knowledge of the IT Regulatory Framework which NABFINS is bound to follow.
 7. Should have experience in Cyber Incidence Response and Co-ordination.
