Sampath Bank
WE PRESENT YOUR FUTURE

MANAGER INFORMATION SECURITY

REQUIREMENTS

- Bachelor's Degree in IT, Cybersecurity, Computer Science, or a related field
- 10 years, out of which 03 years must be at a managerial level, with hands-on experience in Information Security and Compliance
- Experience in working in a Security Operations Centre (SoC) / hands-on experience in monitoring Technology Infrastructure Security, Vulnerability Testing and Mobile Security Testing platforms, and Web Security Testing platforms
- Globally recognised certifications, such as OSCP, CEH, LPT, CISSP, CHFI, etc
- A MSc in Information Security will be considered an added advantage

KEY RESPONSIBILITIES

- Lead and mentor a multidisciplinary cybersecurity team, training, performance management, and resource planning
- Manage the cybersecurity budget, aligning investment decisions with risk priorities and business objectives, while ensuring cost-effective procurement of tools and services, along with the CISO
- Lead the Governance, Risk, and Compliance (GRC) function, conducting enterprise-wide risk assessments, and ensuring full compliance with regulatory obligations
- Conduct Information Security reviews, as per the annual information security plan, and provide a detailed management report and follow-up remediation with relevant parties
- Formulate, implement and identify oversights in policies, strategies and programs designed to manage IS risk
- Co-ordinate with relevant external and internal stakeholders on IT security audits, special application security assessments, vulnerability assessments and penetration tests

- Support the operation and maintain Information Security Management System standard ISO 27001, ISO 27035 and PCI DSS frameworks
- Responsible for implementing and maintaining Security Standard for Information Security Management, as required by the regulator
- Lead Security Operations Centre (SoC) Management, and gather threat intelligence for risk mitigation
- Act as primary contact point for Information Security and Cyber events, investigate security breaches, assess areas of vulnerability and formulate corrective action plans to address issues, along with the CISO
- Evaluate potential business impacts from security breaches and provide strategies and tactical guidance to CISO and higher management
- Co-ordinate with internal and external stakeholders and other interested parties, in the event of an incident, and facilitate evidence management processes of Cyber Security incidents
- Ensure Cyber Security Incident Response Policy is documented, tested and practiced for adequacy, and test Cyber Security Incident Response Capabilities of the Bank in a timely manner

OTHER COMPETENCIES REQUIRED

- Advance knowledge in attack vectors, threat trends, mitigation strategies, intrusion analysis and incident response
- Ability to take on challenges
- Proven track record, with out-of-the-box thinking, and recommending cost-effective security and control solutions
- Ability to multitask
- Good communication skills

An attractive remuneration package, coupled with a modern and conducive work environment, awaits the right candidate. Please apply online, stating qualifications and experience, on or before the 29th of December 2025. Selection will be strictly on merit. Any form of canvassing will be a definite disqualification. Only shortlisted candidates will be contacted.

Click here to apply

Chief Human Resource Officer
Sampath Bank PLC, No. 110, Sir James Peiris Mw., Colombo 02.

Suggestions & Complaints

Supervised by the Central Bank of Sri Lanka | Fitch Ratings 'AA-(lka)'/RWN   📞 1332   🌐 www.sampath.lk

Rise
WITH SAMPATH