Bank of Ceylon is the largest banking institution in Sri Lanka having an island wide branch network with operations in overseas locations including a banking subsidiary in London. We are ranked among the Top 500 banking brands in the world and No.01 in Sri Lanka.

Join Our Information Security Team

We are seeking energetic, innovative, and results-driven professionals to join our Information Security Team and contribute to strengthening the Bank's information security posture, enhancing cyber resilience and support the Bank's business objectives.

Manager – Cyber Resilience (Contract Basis)

Key Responsibilities

- Lead the development, maintenance and testing of the Information Security / Cyber Incident Response Plan (CIRP) and coordinate response efforts during cyber incidents.
- Oversee the integration of cyber resilience into Business Continuity (BCP) and Disaster Recovery (DR) plans. Collaborate with stakeholders to ensure alignment and effectiveness.
- Establish and manage cyber crisis management playbook(s). Conduct tabletop exercises with executives and technical teams.
- Identify vulnerabilities and gaps in the current cyber resilience posture. Recommend risk mitigation strategies.
- Work with IT, Risk, Compliance, Legal, HR, Audit and other Business Units to ensure cyber resilience capabilities meet regulatory, industry and business needs.
- Design and deliver cyber resilience awareness programs for business units and technical teams.
- Ensure alignment with local, foreign and industry regulatory requirements including but not limited to; Related to cyber resilience and incident response
  - o Directions, circulars, and guidelines issued by the Central Bank of Sri Lanka and other regulatory authorities in the countries where BOC operates overseas.
  - o Governing laws, acts, and statutory requirements issued by the Government of Sri Lanka and other relevant regulatory bodies in the countries where BOC has overseas operations.
- Ensure the Bank consistently maintains compliance with PCI DSS and other key information security certifications and frameworks, including ISO 27001 and the NIST Cybersecurity Framework, to uphold industry standards and regulatory requirements.
- Track and report key cyber resilience metrics to executive leadership.
- Perform any other additional duties and responsibilities assigned by the Line Manager in support of organizational security objectives.

Eligibility Criteria

☞ **Should be a citizen of Sri Lanka**

☞ **Qualifications and Experience:**

a) - A degree in one of the following fields, awarded by a university recognized or approved by the University Grants Commission (UGC) of Sri Lanka:
  - o Information Security / Cyber Security,
  - o Computer Science, or Information Technology specialized in Information Security / Cyber Security

- with a minimum of 4 years of experience in cybersecurity, cybersecurity risk management, or Information Systems/Security Auditing including minimum two (2) years of experience in implementing or maintaining PCI DSS and ISO Certification for a financial services sector.

OR

b) - A bachelor's degree in Computer Science or Information Technology, awarded by a university recognized or approved by the UGC of Sri Lanka,

- with a minimum of 5 years of experience in cybersecurity, cybersecurity risk management, or Information Systems/Security Auditing including minimum two (2) years of experience in implementing or maintaining PCI DSS and ISO Certification for a financial services sector.
  - o The ideal candidate should possess strong understanding of cyberthreat and vulnerabilities with familiarity in threat intelligence, SIEM tools, and security operations.

☞ **Professional Qualifications :**

Possession of one of the following professional certifications is preferred

- CISSP – Certified Information Systems Security Professional
- CISM – Certified Information Security Manager
- CRISC – Certified in Risk and Information Systems Control
- SANS/GIAC Certifications (e.g. GCIH, GCPR)
- Certified Ethical Hacker (CEH)

☞ **Required Skills:**

- Leadership & Team Management
- Stakeholder Management, Communication & Coordination
- Analytical & Problem-Solving Skills
- Project Management Skills
- Crisis Management & Resilience Mindset

☞ **Age:** 40 years or below as at the closing date of the application.

Assistant Manager - Incident Response & Security Operation Center (SOC) Services Manager (Contract Basis)

Key Responsibilities

- Oversee daily operations of the outsourced SOC to ensure agreed SLAs and KPIs are met.
- Act as the primary liaison between the Bank and the SOC vendor, ensuring compliance with contractual obligations and timely service reviews.
- Lead end-to-end incident response, coordinating with IT, Risk, Compliance, Legal, and other stakeholders for containment, eradication, and recovery.
- Manage and optimize the corporate SIEM solution, including log integration, correlation rules, and alert tuning.
- Ensure all incidents are recorded, categorized, and reported in accordance with internal policies and regulatory requirements (e.g., CBSL).
- Conduct post-incident reviews, root-cause analyses, and implement continuous improvements.
- Prepare regular SOC performance and incident reports for senior management and relevant committees.
- Drive awareness and training initiatives to strengthen the Bank's cyber resilience culture.
- Develop, maintain, and test incident response playbooks and procedures, including periodic tabletop or simulation exercises.
- Support internal audits, regulatory examinations and risk assessments related to SOC operations and incident management
- Perform any other additional duties and responsibilities assigned by the Line Manager in support of organizational security objectives.

Eligibility Criteria

☞ **Should be a citizen of Sri Lanka**

☞ **Qualifications and Experience:**

a) - A degree in one of the following fields, awarded by a university recognized or approved by the University Grants Commission (UGC) of Sri Lanka:
  - o Information Security / Cyber Security,
  - o Computer Science or Information Technology specialized in Information Security / Cyber Security,

- with a minimum of three (03) years of experience in information/cybersecurity, technology risk management or information systems/security auditing including at least one (01) year of direct experience in SOC operations and incident response, preferably in a banking or financial services environment

OR

b) - A bachelor's degree in Computer Science or Information Technology, awarded by a university recognized or approved by the UGC of Sri Lanka,

- with a minimum of four (04) years of experience in information/cybersecurity, technology risk management, or information systems/security auditing including at least one (01) year of direct experience in SOC operations and incident response, preferably in a banking or financial services environment.
  - o The ideal candidate should possess Strong expertise in SIEM platforms, threat detection, and incident response, with a proven ability to manage third-party security providers and vendor SLAs.

☞ **Professional Qualifications :**

Possession of one of the following professional certifications is preferred:

- GIAC Certified Incident Handler (GCIH)
- Certified Information Systems Security Professional (CISSP)
- Certified Information Security Manager (CISM)
- Computer Hacking Forensic Investigator (CHFI)
- Certified Ethical Hacker (CEH)

☞ **Required Skills:**

- Leadership & Team Management
- Stakeholder Management, Communication & Coordination
- Analytical & Problem-Solving Skills
- Project Management Skills
- Crisis Management & Resilience Mindset

☞ **Age :** 32 years or below as at the closing date of the application.

Terms and Conditions

- Fixed Term Contract for a period of 03 years; performance will be reviewed annually.
- Negotiable, attractive remuneration package will be offered based on the candidate's profile

Selection Procedure

Shortlisted candidates based on the above eligibility criteria will be selected by an interview process.

Application Procedure

Send your complete and updated Curriculum Vitae with comprehensive details of your qualifications, experience, professional certifications by e-mail to careers@boc.lk, mentioning the post you have applied for on the Subject line of the e-mail to reach us on or before 11.07.2026.

Any application not meeting the above required eligibility criteria as at the closing date or received after closing date or fail to provide the relevant supportive documents at the interview to prove the fulfilment of the above eligibility criteria will be rejected/ disqualified at any stage of the recruitment without any further notice.

All the prospective applicants are expected to read the Bank's "Personal Data Protection Notice for Recruitment" which is available in the Bank's website under HR Management page (https://www.boc.lk/hr-management) and acknowledge the same in the e-mail when applying for the vacancy.

Deputy General Manager (Human Resource Operations)
Human Resource Division
Bank of Ceylon
Colombo 01

- *Any form of canvassing will lead to immediate disqualification.*
- *The Bank reserves the right to call only the short-listed candidates.*
- *The Bank reserves the right to postpone / cancel the recruitment.*
- *The Bank protects the privacy and confidentiality of your information as per the Personal Data Protection Policy of the Bank.*