

ELEVATE YOUR SPIRIT
**GROW YOUR
CAREER**

Assistant Manager IT Security

We are looking for a dedicated and proactive individual to join our IT Security team. In this role, you will play a critical part in protecting our systems, data, and digital assets by supporting proactive threat detection, vulnerability management, and incident response initiatives.



Job Responsibilities

- Assist in executing cybersecurity Governance, Risk, and Compliance (GRC) activities to ensure strict adherence to CBSL, SWIFT, PCI, and internal security requirements
- Perform daily monitoring, response and threat detection activities utilizing SIEM/SOC tools to ensure comprehensive system coverage
- Manage daily Identity and Access Management (IAM) processes, including conducting periodic access reviews for privileged and critical systems
- Execute daily vulnerability management operations, ensuring high levels of patch compliance across servers, endpoints, and infrastructure
- Conduct and coordinate periodic Vulnerability Assessments and Penetration Testing (VAPT) across web applications, mobile apps, APIs, and network infrastructure
- Review, evaluate, and approve firewall rule change requests to ensure strict compliance with network security policies and least-privilege access principles
- Assist in conducting comprehensive security assessments of third-party vendors and service providers prior to onboarding
- Assist in managing internal and external security audits by tracking and ensuring the timely closure of findings
- Compile data for security posture reports and track Key Risk Indicators (KRIs) for management review



Experience & Qualifications

- Bachelor's Degree in Information Security, Cybersecurity, Computer Science, or a related IT discipline
- Minimum of 6-8 years of hands-on experience in IT Security operations. Prior work experience in the Banking and Financial Services sector will be a distinct advantage
- Demonstrated expertise in Security Monitoring, Threat Detection, and Incident Response (SOC/SIEM)
- Solid practical understanding and hands-on experience with or working knowledge of major NGFW vendor platforms (e.g., Palo Alto Networks, Fortinet, FortiGate, Check Point)
- Strong capability in Cybersecurity Governance, Risk & Compliance (GRC) frameworks
- Proficiency in Vulnerability Management, Security Testing, and Patch Management
- Solid practical experience in Identity & Access Management (IAM) and Privileged Access Control
- Understanding of Third-Party and Vendor Security Risk Management practices
- Industry-recognized cybersecurity certifications (e.g., CCNP, PCNSA/PCNSE, NSE5 or above, OSCP, CEH, or working towards CISA/CISM/CISSP) are highly advantageous

Interested candidates are invited to forward their CVs to career@cargillsbank.com mentioning the post applied for, in the subject line of the email on or before **29th October 2026**.

Head of Human Resources

Cargills Bank PLC,

No. 696, Galle Road, Colombo 03. Tel. 011 7 640 640



Fitch Rating A(Ika)

www.cargillsbank.com f @in v d

Cargills Bank PLC is a licensed commercial bank supervised by the Central Bank of Sri Lanka

SINCE 2014

Gazette

AMBITIONS REALIZED



CargillsBank
BANKING ON THE HUMAN SPIRIT