Vacancy Announcement

FTB
ធនាគារពាណិជ្ជកម្មក្រៅប្រទេស នៃកម្ពុជា
Foreign Trade Bank of Cambodia

Exciting Career Opportunity

Foreign Trade Bank of Cambodia (FTB) is the first commercial bank in Cambodia, a truly local bank trusted since 1979. FTB has been providing customers with safe and reliable banking services. With the vision to be the preferred commercial bank in Cambodia, we continue supporting customer to grow and prosper while offering stable and long term career opportunities for all staff. As we are expanding the operation and building a high performing team to support our long-term sustainable growth, we are looking for highly motivated and qualified candidates to join with our "Employer of Choice Bank"

Manager, IT Secuity Testing Unit (1 Position based in Head Office)

The Manager, IT Security Testing Unit leads FTB's security testing program to identify, validate, prioritize, and report technology and cyber risks across banking systems, infrastructure, digital channels, applications, APIs, payment/card environments, and third-party technology services. The role manages vulnerability assessment, penetration testing, application security testing, mobile/API testing, segmentation testing, adversarial attack simulation coordination, retesting, remediation tracking, and management reporting. The role must ensure testing is performed safely, ethically, and within approved scope, rules of engagement, test windows, data protection requirements, and regulatory expectations.

***Main Duties:**

- Develop, maintain, and execute the Bank's annual IT security testing plan covering applications, infrastructure,
- network, mobile, API, digital banking, payment systems, and critical technology environments.
- Lead internal security testing activities within approved scope, test window, rules of engagement, change coordination, data protection requirements, rollback plans, and escalation procedures.
- Conduct and/or supervise vulnerability assessments and penetration testing to identify security weaknesses in systems, applications, networks, and banking technology platforms.
- Define security testing methodology, test scope, risk rating criteria, acceptance criteria, evidence requirements, and reporting format for each engagement.
- Coordinate and lead external penetration testing, red team/adversarial simulation, PCI DSS testing, SWIFT-related testing, and other independent security assessment projects.
- Validate and retest identified vulnerabilities after remediation to confirm effective closure and reduce repeat findings.
- Track, report, and escalate remediation progress for vulnerabilities, including overdue, repeated, high-risk, and critical findings.
- Maintain proper security testing records, including test scope, evidence, findings, risk rating, remediation action, retest result, closure status, and management approval where required.
- Prepare and present technical and executive-level reports to management, IT Risk Committee, system owners, application owners, and relevant stakeholders.
- Support compliance with NBC TCRMG, PCI DSS, SWIFT CSP, ISO 27001, OWASP, and internal IT security policies and procedures.
- Review security testing results from internal teams, external vendors, auditors, regulators, and third-party service providers.
- Work with system owners, application owners, infrastructure teams, digital banking teams, and vendors to ensure timely remediation of security weaknesses.
- Provide security testing advice for new systems, applications, digital banking services, infrastructure changes, and technology projects before production deployment.
- Monitor emerging threats, attack techniques, exploit trends, vulnerabilities, and security testing tools relevant to the Bank's environment.
- Develop and improve security testing procedures, checklists, templates, testing standards, reporting formats, and key performance indicators for the unit.

***Skill/Requirement :**

- Bachelor's degree or equivalent in Computer Science, Information Technology, Cybersecurity, Software Engineering, or related field.
- Professional certification is strongly preferred: OSCP, eCPPT, CEH/CPENT, eJPT, or equivalent penetration testing / application security certification.
- Minimum 5 years of cybersecurity experience, including at least 3 years in vulnerability assessment, penetration testing, application security testing, or security control assessment.
- At least 3 years of team leadership, project coordination, vendor management, or management reporting experience is preferred.
    - Banking, financial services, payment/card, SWIFT, or digital banking experience is strongly preferred.