Phillip Bank Plc is a member of PhillipCapital based in Singapore. PhillipCapital established since 1975 is an Asian integrated financial house providing a wide range of products and services with presence in 15 countries, including offices in Australia, Cambodia, China (and Hong Kong SAR), France, India, Indonesia, Japan, Malaysia, Singapore, Thailand, Turkey, UK, UAE, USA and Vietnam. PhillipCapital manages total asset of USD35 Billion with shareholder's fund in excess of USD1.5Billion as of 2018.

Phillip Bank Plc has been established in Cambodia as a commercial bank since 2014. After its merger with Kredit Microfinance in 2020 we currently provide our banking services throughout the Kingdom of Cambodia through our network of over 89 branches.

We aim to build convenient, integrated, innovative, and trusted financial solutions by leveraging technology platforms and engaging our staff, business partners, and customers to sustainably improve the economic well-being of families in rural and urban communities.

To support the bank’s expansion plans, we are seeking dynamic candidates to join our team as following:

<table>
<thead>
<tr>
<th>Location/Province</th>
<th>Department/Branch</th>
<th>Positions</th>
<th>Vacancies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Head Office</td>
<td>IT Department</td>
<td>Senior Officer, IT Security and Compliance</td>
<td>01</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IT Security Specialist, Pentest</td>
<td>01</td>
</tr>
</tbody>
</table>

1. Position: Senior Officer, IT Security and Compliance

**Job Responsibilities**
- Provide the excellent supports on overall aspects of Information Security, IT Governance, IT Risk, IT Audit and IT Compliance;
- Perform IT risk assessment and produce actionable plan to secure bank’s application, data and networks.
- Monitoring network usage to ensure compliance with security policies.
- Assess and develop up to date with IT security policy, standards and threats.
- Collaborate with management and the related IT department to improve security posture.
- Document any security breaches and assessing their damage.
- Coordinate and update information security incident response document, ensuring processes and procedures are tested regularly in line with IT continuity, business continuity planning (BCP) and disaster recovery (DR) policy;
- Promote cyber security awareness posture at all levels of management and employees, by maintaining and developing a positive culture of compliance against IT security policy, industry standards and regulations;
- Identify and address a full range of issues from structure and policy, through to assisting in specific areas such as data privacy; data leakage prevention / monitoring; information rights management; third party security and cryptography;
- Perform day to day IT security operation required by head of departments and management.
- Minimize all risks including operational, information and cyber security risk;

**Job Requirements**
- Having 3 years of experiences within IT security related domain and working in financial / telecom / auditing industry.
- Bachelor's Degree in Information Technology, Computer Science, and Software Engineering or a related qualification, and/or demonstrated capability through past employment experience;
- Holding any IT security related certification (ISO27001 LI, CEH, CCNA / CCNP Security) or from equivalent recognized organizational body is a plus.
- Proven experience of implementing an information security management system (ISMS);
- Experience in undertaking internal and third party audits covering IT governance and information security controls;
Solid understanding of IT and experience in developing IT governance, controls and best practices;
Proven ability to write easy to understand reports and deliver presentations on information risk management, systems process control and IT general control review reports;
Proven ability to author and revise information security policies and procedures;
Proven ability to work and communicate effectively and fluently with managers and staff, including the ability to explain complex technical issues in terms that non-technical managers and staff will understand;
Have a strong understanding of advanced threat detections, continuous vulnerability assessment, response and mitigation strategies used in Cyber Security operations;
An understanding of a business continuity role and/or policies processes and plans;

2. Position: IT Security Specialist, Pentest

Job Responsibilities
- Provide the excellent supports on overall aspects of Information Security, IT Governance, IT Risk and IT Assurance.
- Operate a hands-on role involving penetration testing and vulnerability assessment activities of applications, operating systems, networks, and mobile applications on regularly basis to identify vulnerability across several systems.
- Analyze security policies configuration and provide recommendation based on industry best practices.
- Produce actionable, threat-based, reports on security testing results and present the finding to head of department and management ongoing basis.
- Conduct physical assessments of servers, systems, and network device security.
- Coordinate and lead on external and internal penetration testing projects and provide promptly update to management
- Consult with application developers, systems administrators, and management to demonstrate security testing results, explain the threat presented by the results, and consult on remediation
- Promote information governance and security at all levels of management and employees, maintaining and developing a positive culture of compliance against industry standards and regulations;
- Identify and address a full range of issues from structure and policy, through to assisting in specific areas such as data privacy; data leakage prevention / monitoring; information rights management; third party security and cryptography;
- Develop and maintain security assessment testing plans.

Job Requirements
- Having 2 years of experiences on network, application or mobile pentest and security configuration review or working experiences in financial / telecom / auditing industry.
- Bachelor's Degree in Information Technology, Computer Science, and Software Engineering or a related qualification, and/or demonstrated capability through past employment experience;
- Holding security related certification (CySA+, CHFI, OSCP, OSCE) or from equivalent recognized certification body.
- Proven ability to write easy to understand reports and deliver presentations on information risk management, systems process control and IT general control review reports;
- Proven ability to work and communicate effectively and fluently with managers and staff, including the ability to explain complex technical issues in terms that non-technical managers and staff will understand;

PhillipBank provides competitive salary (based on experience and performance) and benefits as follows:
1. Sales Incentive & Annual Bonus
2. Pchum Ben Bonus
3. 13th Month Salary
4. Personal Accident & Term Life Insurance
5. Outpatient Consultation & Treatment
6. Public Holidays follow Labor Law
7. 5 Working days per week.
8. Staff Loans with special interest rate
9. Training & Development Opportunities

How to apply
Interested candidate should submit ONLY their CV with a cover letter to: Head Office at #27DEF, Monivong Blvd, Sangkat Srah Chork, Khan Daun Penh, Phnom Penh by Email: careers@phillipbank.com.kh Or candidates can apply by Website: www.phillipbank.com.kh (Send only CV & cover letter in word or pdf file. Don’t attach docs).

Closing Date: 30 June 2020 at 04:00 PM

PhillipBank adheres to the principle of recruitment that is unbiased, transparent, non-discriminatory towards sex, religious, political affiliation, disability, color and marital status.

Note: Only shortlisted candidates will be notified. The application and documents will not be returned.