Specification of Competency Standards for the Retail Banking

Unit of Competency

Technology Management > 5.1 Information and Cyber Security

Title	Conduct audits to assess effectiveness on cyber security risk protection and carry out incident monitoring and reporting
Code	107427L4
Range	Provide management of the bank with an independent assessment relating to the effectiveness of cybercrime prevention, detection and incident management processes, policies, procedures and governance activities
Level	4
Credit	3
Competency	Performance Requirements 1. Is knowledgeable in the new development; apply latest technologies and industry best practices to design cyber security audit Be able to: • Assess the development in cyber security and is knowledgeable in latest technologies and industry practices • Apply the best practices to conduct a detailed assessment with a focus on cybercrime management standards, guidelines and procedures as well as the implementation and governance of these activities • Lead and execute cyber security audit in alignment with other operational audits of the incident management process, configuration management and security of networks and servers, security management and awareness, business continuity management, information security management, governance and management practices of both IT and the business units, and relationships with third parties. 2. Analyse systems of the bank and identify potential vulnerabilities Be able to: • Analyse the bank's systems for potential vulnerabilities that result from poor or improper system configuration, known and / or unknown hardware or software flaws, or operational weakness • Identify specific vulnerabilities and provide detailed instructions to mitigate or eliminate each risk • Design and implement "cyber defense" independent review of security measures and performance; assess and identify opportunities to strengthen enterprise security 3. Conduct overall cyber risk audit and report to management team of the bank Be able to: Be able to: • Conduct a comprehensive cyber risk assessment for the bank and distill the findings into a concise summary for the audit committee and management team which can drive a risk-based cybersecurity audit plan. • Evaluate the full cyber security framework; compare current state against framework characteristics where the bank is aiming at, and the expected cyber security practices across the banking industry • Honestly report deficiency and shortcomings of existing systems based on cyber risk assessment excises; accept constructive feedback and seek improvement measures proactively
Assessment Criteria	The integral outcome requirements of this UoC are: • Lead and conduct comprehensive audit to assess cyber security effectiveness of the bank regularly and submit reports to management team for improvement and future audit planning
Remark	