Specification of Competency Standards
for the Banking Industry
Unit of Competency

Functional Area - 6. Technology Management
(Key Function – 6.2 IT System Security/ Cybersecurity)

Title	Assess effectiveness on cybersecurity risk protection and carry out incident monitoring and reporting
Code	109375L4
Range	Assessment of the overall effectiveness of the bank's cybersecurity risk protection and reporting structure; including the provision of management information to the bank with an independent assessment relating to the effectiveness of cybercrime prevention, detection and incident management processes, policies, procedures and governance activities. This entails the assessment of different systems in Artificial Intelligence (AI), Blockchain, Big Data collection and analytics, etc.
Level	4
Credit	3 （For Reference Only）
Competency	Performance Requirements 1. Knowledge in the Subject Area Be able to: • Possess knowledge in latest technologies and apply it to assess the development in cybersecurity; • Comprehend the industry practices in cybersecurity and apply the best practices to conduct a detailed assessment on cybercrime management standards, guidelines and procedures as well as the implementation and governance of these activities. 2. Applications 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; • Execute cybersecurity 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; • Design and implement "cyber defence" independent review of security measures and performance; assess and identify opportunities to strengthen enterprise security. 3. Professional Behaviour and Attitude Be able to: • Conduct a comprehensive cyber risk assessment for the bank and distil the findings into a concise summary for the audit committee and management team which can drive a risk based cyber-security audit plan; • Evaluate the full cybersecurity framework; compare current state against framework characteristics where the bank is aiming at, and the expected cybersecurity practices across the banking industry; • Report deficiency and shortcomings of existing systems honestly based on cyber risk assessment exercises; accept constructive feedback and seek improvement measures proactively.

Specification of Competency Standards
for the Banking Industry
Unit of Competency

Functional Area - 6. Technology Management
(Key Function – 6.2 IT System Security/ Cybersecurity)

Assessment Criteria	The integral outcome requirements of this UoC are: • Following the bank's standard procedures to conduct comprehensive audit to assess cybersecurity effectiveness of the bank regularly and submit reports to management team for improvement and future audit planning.
Remark	