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 and manage security risks and trends in digital and mobile environment
Code	109369L5
Range	Implementation of bank-wide cyber risk assessment and management initiatives to conduct data analysis for the purpose of identifying trends of security risks in digital, mobile and other IoT environment. This covers the accountability of developing technology deployment plans to ensure that cyber-security technology adopted by the bank are operationally effective, upgraded and enhanced to meet the changing threat setting and business requirements.
Level	5
Credit	4 （For Reference Only）
Competency	Performance Requirements 1. Knowledge in the Subject Area Be able to: • Possess the knowledge of technological development in the banking industry and evaluate the trend in cybersecurity; • Master the knowledge in utilizing tools and techniques to tackle cyber risks and apply it to design, deploy and maintain bank-wide cyber risk management methodologies; • Be familiar with the bank's IT systems and use the knowledge to assess bank-wide business risks and cyber threats; hence to develop detailed business risk scenarios and cyber threat models. 2. Applications Be able to: • Use of tools and technology to provide data analytics and business intelligence on cyber threats, risks and vulnerabilities; • Develop, implement and conduct periodic testing of cyber resiliency plans to cope with the changes in the trend of cyber risks; • Manage and oversee large projects involving information security, technology risk management, and cybersecurity or cyber risk management to ensure the projects are smoothly implemented. 3. Professional Behaviour and Attitude Be able to: • Protect customer and employee confidential information, and take steps to ensure all initiatives are in compliance with regulatory and audit requirements; • Monitor and report of trends of risks, threats and vulnerabilities in digital and mobile platforms; follow up to take remedy actions with an aim to enhance risk management effectiveness; • Recommend improvement on technology deployment plans of the bank to ensure cybersecurity technology adopted can meet the changing threat environment and business needs.
Assessment Criteria	The integral outcome requirements of this UoC are: • Assessment of bank-wide business risks and cyber threats; solutions delivered are able to address the needs of all business and operational functions of the bank.
Remark	