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	Design and implement cybersecurity awareness education and employee training
Code	109370L5
Range	Promotion and of cybersecurity awareness and implementation of education programmes for both employees and customers. This refers to on-going and ad-hoc education programmes offered to employees, clients, business partners and other stakeholders.
Level	5
Credit	4 （For Reference Only）
Competency	Performance Requirements 1. Knowledge in the Subject Area Be able to: • Possess the knowledge in the development of cybersecurity and apply it to identify the needs to foster cybersecurity awareness of different parties; • Understand the importance of IT risk awareness education and promote stakeholders' awareness of computer risks and cybersecurity as well as the risks associated with related digital platforms linked up with the bank; • Understand the work related to cybersecurity conducted by different parties and based on that to enhance cooperation with financial services industry practitioners and law enforcement agencies to exchange intelligence in technology crime and cybersecurity. 2. Applications Be able to: • Develop and implement cyber risk information sharing programmes and widely disseminate the messages to related parties; • Produce educational and promotional materials related to cybersecurity, such as posters, leaflet, booklets, video, etc. to promote the initiative; • Establish guidelines and information tool to educate employees and customers to conduct health checks on their computers, mobile devices and websites and enhance awareness on possible cyber-attacks. 3. Professional Behaviour and Attitude Be able to: • Develop comprehensive contents of training consist of collection of preventive tools, policies, security concepts, security safeguards, guidelines and risk management approaches; • Establish physical and online learning centres for employees and other stakeholders to learn about the security risks they should be aware of and the precautions they can take.
Assessment Criteria	The integral outcome requirements of this UoC are: • Building cybersecurity education infrastructure and instil a culture to combat cyber-crimes; • Establishment of conventional and online training curricular on cybersecurity.
Remark	