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	Educate business users on information and cyber risk trend and controls in a banking environment
Code	109373L5
Range	Conducting research to develop and/or revise training courses, communication sessions, briefing workshops and/or independent educational interactive meetings for enterprise banking clients. This includes the preparation of appropriate educational materials, and/or conducting formal classroom courses and workshops.
Level	5
Credit	4 （For Reference Only）
Competency	Performance Requirements 1. Knowledge in the Subject Area Be able to: • Have an in-depth understanding of different concepts, terms, processes, policy and implementation of information and cybersecurity; • Possess the knowledge in the trend and control of information and cyber risk and apply it to access to and compare the latest security measures at all stages of an information system life cycle; • Keep up to date on the development of information and cybersecurity, as well as using this knowledge to solve complex problems involving a wide variety of information systems. 2. Applications Be able to: • Plan, organize and manage the presentation of major risk trend and controls on cybersecurity. Assigns training classes or communication sessions to instructors and evaluates instructor training effectiveness; • Conduct comprehensive reviews of learning courses and programmes, evaluate the impact of planned or projected changes in cybersecurity trend on associated training requirements; • Develop and maintain presentations, audios, videos and security content in support of the communication strategy for cybersecurity education and awareness; • Review and revamp existing education programme content in accordance to changed cyber risk trend; • Establish and maintain uniform understanding and application of Business Continuity Plans, processes and solutions before the drilling test; • Monitor implementation and integration recovery process for affected business and operations areas. 3. Professional Behaviour and Attitude Be able to: • Develop and execute strategies, methodologies, communication campaigns and training plans to develop and foster a culture of cybersecurity, privacy, and continuity across the bank’s client organizations; • Design communication sessions and workshops with a central focus on driving clients’ alertness and organizational change towards a culture that focuses on information and cyber secure practices.

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: • Delivery of effective educational and/or awareness programmes on cybersecurity and risk control for enterprise banking clients; • Formulation of effective training, education and communication strategies and implementation plans including analysis, execution, testing and documentation are established to create impact to clients' organization culture on cybersecurity and controls.
Remark	