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	Formulate IT and cybersecurity policies, roadmaps and strategies
Code	109366L6
Range	Design of policy on IT security for protecting the bank from unauthorized access, alteration, unauthorized disclosure, etc. This covers all IT and financial technology systems of the bank regardless of the business or operations functions.
Level	6
Credit	4 （For Reference Only）
Competency	Performance Requirements 1. Knowledge in the Subject Area Be able to: • Recognise the changes in IT and financial technology in the banking industry and the wider market, and apply the knowledge to analyse future trends and developments in IT security threats and measures based on incomplete information collected from different sources; • Understand the compliance requirements and based on that to determine regulatory requirements and obligation under different jurisdictions; • Understand the business requirements of key stakeholders and apply the knowledge to analyse views collected from different business and operation units accurately to discern their needs in IT control or security (e.g. network). 2. Applications Be able to: • Establish strategic objectives and compliance position for IT security of the bank in order to provide protection with an outlook of future perspective; • Establish IT control or security (e.g. network) policies with respect to the bank's business strategies and security needs; • Develop implementation plans with different parties to ensure smooth running in service delivery and daily operations while complying with the bank's security policies. 3. Professional Behaviour and Attitude Be able to: • Direct communication and education programs on IT security measures; ensure all levels of staff are aware of their importance and participate in the protection of information security; • Design monitoring measures to ensure compliance with established security policies in order to protect the bank against unauthorized access, alteration, unauthorized disclosure, etc.
Assessment Criteria	The integral outcome requirements of this UoC are: • Formulation of security policies. The policies should be based on critical analysis of a broad range of data and incomplete information with the aim to provide enough protection to bank's IT systems and meet the regulatory requirements without hampering operational efficiency; • Production of supporting measures on enforcing security policies. Comparison of different types of security measures should be provided to support the design.

Specification of Competency Standards
for the Banking Industry
Unit of Competency

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

Remark	