Specification of Competency Standards
for the Banking Industry
Unit of Competency

Functional Area - 6. Technology Management
(Key Function – 6.4 IT Operations and Support)

Title	Perform incident response management for IT, digital banking and financial technology issues
Code	109391L5
Range	Management of incidents in IT, digital banking, Artificial Intelligence (AI), Blockchain, Big Data, etc. systems. This applies to different kinds of incidents arising in different types of IT and financial technology systems.
Level	5
Credit	4 （For Reference Only）
Competency	Performance Requirements 1. Knowledge in the Subject Area Be able to: • Possess knowledge in different technology systems and apply it to detect and identify security incidents; • Master the technical knowhow of technology related incidents analysis and apply the knowledge to review security incidents; • Possess the knowledge in causes identification related to IT issues and apply it to collect necessary data related to the incidents in order to find out the truth and conduct investigation on technology security and root cause analysis. 2. Applications Be able to: • Direct contingency or recovery plan for minimizing damages of technology security incidents promptly; • Devise response procedures for the incidents in order to formulate general solutions to tackle security issues in the long run; • Oversee the writing of reports on technology security incidents for record and documentation. 3. Professional Behaviour and Attitude Be able to: • Respond to any report of security violations and carry out investigation to diagnose the causes in a professional manner; • Conduct post-mortem review and follow up as well as carry out necessary remedial actions to ensure security of the bank systems or databases.
Assessment Criteria	The integral outcome requirements of this UoC are: • Investigation on security incidents in order to find out the causes. The investigation should be based on the analysis of the data collected; • Recommendation of solutions to contain the damage caused by the incident. These should be based on evaluation on findings from investigation and analysis on information from different sources.
Remark	