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	Carry out IT system security / cybersecurity incident investigation, monitoring and reporting
Code	109374L5
Range	Investigation of IT related security issues and cybersecurity incidents for the bank and collect evidence. This refers to all kinds of systems risks across different business / operations units of the bank.
Level	5
Credit	4 （For Reference Only）
Competency	Performance Requirements 1. Knowledge in the Subject Area Be able to: • Understand forensics concepts and investigation techniques and apply the knowledge to evaluate different issues in IT and cybersecurity in order to develop the framework of investigation plan; • Possess knowledge in investigation methodologies and based on that to evaluate different investigation approaches in order to develop the procedures in conducting investigation of security cases; • Demonstrate professional knowledge in the various techniques in evidence gathering. 2. Applications Be able to: • Identify the case for investigation, provide logistical, technical and exploratory support to IT system security / cybersecurity incident detection; • Develop investigation plan that define the procedures and techniques used in information collection and documentation of forensic activities; • Examine the collected data and recognize essential elements of possible forensic activities; • Preserve evidence collected for internal investigation or law enforcement agencies' follow up; • Aggressively investigate systems forgery and fraud related crimes and incorporate the cooperative efforts of other law enforcement agencies to meet this goal; • Write up incident reports and record lessons learnt from IT system security / cybersecurity incidents. 3. Professional Behaviour and Attitude Be able to: • Investigate security case in a professional manner with an aim of playing a role in the prevention, investigation and prosecution of system related financial crimes to protect the bank's information and enhance public safety; • Define guidelines and ensure that steps taken during investigation are in accordance with the bank's policies and any laws and regulatory requirements.
Assessment Criteria	The integral outcome requirements of this UoC are: • Investigation of the security case in a professional manner; • Preservation of evidence for later internal analysis and / or police investigation.
Remark	