Specification of Competency Standards
for the Information & Communications Technology Industry
Unit of Competency

Functional Area - Information Security

Title	Conduct investigation of Information Security Incidents
Code	111169L5
Range	This UoC involves Investigating information security issues for the organisation, collecting evidences and documenting the activities conducted
Level	5
Credit	3 （For Reference Only）
Competency	Performance Requirements 1. Understand forensics concepts and investigation techniques for the IT systems involved • Be able to: o Evaluate different issues in IT security in order to develop the framework of investigation plan o Evaluate different investigation approaches in order to develop the procedures in conducting an investigation of security cases o Demonstrate professional knowledge in the various techniques in evidence gathering o Understand the functions and operations of the systems involved in the incident 2. Investigate security case in a professional manner • Be able to: o Identify the case for investigation, define guidelines and ensure that steps taken during investigation are in accordance with the company's policies and any laws and regulatory requirements o Develop investigation plan that define the procedures and techniques used in information collection and documentation of forensic activities o Examine the collected data and recognize essential elements of possible forensic activities
Assessment Criteria	The integral outcome requirements of this UoC are the abilities to： • Investigation of the information security case in a professional manner • Documentation of conducted activities • Preservation of evidence for later internal analysis and/ or police investigation
Remark	