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

Functional Area - Information Security

Title	Design the digital forensic process in terms of technical and legal aspects
Code	111167L6
Range	Design the process to carry out digital forensic investigation of cyberattacks. The procedures should adhere to the organization's policies and oblige the associated jurisdictions
Level	6
Credit	3 （For Reference Only）
Competency	Performance Requirements 1. Possess the knowledge in the subject area • Understand the needs, importance and the limitation of digital forensic • Know of the tools needed for conducting digital forensic investigation • Understand the processes and the latest technological development in data recovery • Recognise the changes in IT technologies and how they could impact digital forensic • Understand the laws that are associated with the organization's business operations and digital forensic 2. Design the process • Establish the procedures to identify evidence and the location they are stored • Create a set of guidelines in isolating, securing and preserving the data to prevent possible tampering • Set up the protocol for data reconstruction/recovery and data analyses for drawing conclusion of the attack • Formulate a system for documenting all the associated data, evidence and procedure • Establish the procedure to summarise the data, such that non-IT personnel, for example, lawyer and the judge, could have a basic understanding of the impact and ramifications of the incident • Ensure all procedures carried out adhered to organization's policies and obligated to the associated jurisdictions
Assessment Criteria	The integrated outcome requirements of this UoC are： • Design the digital forensic process. The process should cover evidence identification, data preservation, data analysis and documentation. • All procedures should adhere to the organization's policies and oblige to the associated jurisdictions
Remark	