Information and Communications Technology Industry Training Advisory Committee
Software Products and Software Services (SW) branch
Unit of Competencies

1. Title	Investigate an information security case
2. Code	ITSWIS517A
3. Range	Investigate an ICT-security case for an organization with presentable evidence [Information Security – Forensics]
4. Level	5
5. Credit	5
6. Competency	Performance Requirement 6.1 Understand the knowledge of forensics concepts and investigation techniques — Be able to ▪ understand ICT-security issues ▪ understand the procedures in conducting an investigation on security cases ▪ understand the various techniques in evidence gathering ▪ apply forensics principles to an assessment environment ▪ understand the framework of an investigation plan 6.2 Identify a case for investigation — Be able to ▪ define a set of guidelines for identifying a case ▪ ensure that steps taken during investigation are legal within the law ▪ evaluate whether a case is suitable for investigation 6.3 Develop an investigation plan — Be able to ▪ define the procedures for handling an investigation on a particular case ▪ define the techniques used in information collection ▪ determine the policies, procedures, processes and types of tools ▪ designate staff with knowledge to handle the investigation ▪ define the framework in documenting all forensics activity 6.4 Examine the collected data — Be able to ▪ designate staff to conduct forensics analysis ▪ understand and interpret the collected data and preparing evidence for civil litigation ▪ collate useful information and admissible evidence from collected data ▪ be able to recognize essential elements of possible offending 6.5 Investigate a security case professionally — Be able to carry out an investigation to security cases in accordance with the organization's guidelines as well as any (local and international) laws and regulatory requirements, if applicable
7. Assessment Criteria	The integrated outcome requirements of this UoCs are the abilities to: (i) formulate a set of guidelines to identify a security case ; and (ii) develop a plan to investigate an ICT-security case.
Remark	