

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

1. Title	Devise processes for detecting, identifying and analysing security incident	
2. Code	ITSWIS613A	
3. Range	Develop and implement processes for detecting, identifying and analysing security related events for an organization to support its normal business operations away from security threats [Information Security – Response Management]	
4. Level	6	
5. Credit	2	
6. Competency	<p>6.1 Understand help desk processes</p> <p>6.2 Know information security incident detection and reporting policies and processes</p> <p>6.3 Develop processes to deal with security incidents</p> <p>6.4 Develop processes to deal with security incidents professionally</p>	<p><u>Performance Requirement</u> Be able to</p> <ul style="list-style-type: none"> ▪ identify security incidents reported by users (Being able to identify something assumes the ability to distinguish something from others.) ▪ explain the reason why some help desk issues are security incidents and others are not <p>Be able to develop processes for detecting and identifying information security incidents</p> <p>Be able to develop and implement processes for detecting, identifying and analysing security related events of an organization</p> <p>Be able to develop and implement processes for detecting, identifying and analysing security related events in compliance with organization's guidelines as well as any (local and international) laws and regulatory requirements, if applicable</p>
7. Assessment Criteria	The integrated outcome requirements of this UoCs are the abilities to: (i) develop and implement organizational processes for detecting, identifying and analysing security related events; and (ii) ensure that the developed and implemented processes comply with the organization's policies and guidelines and any applicable local and international laws and regulatory requirements.	
Remark		