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

1. Title	Define operational security protection processes	
2. Code	ITSWOS522A	
3. Range	Define process for security control to protect the system from security threats in accordance with security control policy in the context of providing security management services for the IT operations of an organization [Operations and Support – Security Management Services]	
4. Level	5	
5. Credit	2	
6. Competency		Performance Requirement
	6.1 Understand security control requirements and types of security threats	Be able to ▪ digest the security policy and guidelines from management ▪ comprehend the security control plan ▪ identify different types of security threats to business processes
	6.2 Define process to protect the infrastructure from security threats	Be able to ▪ define process and measures to protect the infrastructure from security threats ▪ recommend the appropriate anti-virus software (signatures) and security patches
	6.3 Monitor, investigate and perform corrective actions in accordance to security control policy	Be able to ▪ monitor alerts and reported exceptions ▪ investigate the alerts to determine the root cause ▪ carry out corrective actions in accordance to security control policy
	6.4 Define process for security control in accordance to security control policy professionally	Be able to ▪ locate reliable support sources with current information on security threats for collaboration and mutual support ▪ exercise industry best practices and adhere to standards as well as local and international standards ▪ comply with organization's guidelines and procedures 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) define process to protect the infrastructure from security threats; and (ii) monitor, investigate and perform corrective actions in accordance to security control policy.	
Remark	1. Examples of security threats include, but are not limited to, virus attacks, unauthorised intrusion and security breach. 2. The participant is assumed to have a comprehensive knowledge in IT and its applications. 3. This UoCs comprises both planning and operating the security for infrastructure environment for the security management services of ITIL®.	