Vocational Qualifications Pathway (VQP) for Information Security

Job Area / Job Level	Information Security
Master Level	*The ICT practitioners at this level mainly responsible for decision-making processes. They oversee the entire IT operations and strategic development direction in the organization. Professionals at this level require broad corporate perspective, good communication skills and great technology knowledge.*
Job Title	Chief Information Security Officer
	Information Security Director
Specialist Level	*The ICT practitioners at this level mainly involve in managerial processes. They may associate with individual technical departments and manage those departments by applying their technical and managerial skills. The major tasks performed by the professionals at this level is to manage the individual activities and project segments to lead the project towards completion within the assigned budget and stipulated deadline.*
Job Title	Information Security Architect
	Information Security Engineer
	Information Security Analyst
	Cryptographer
Practitioner Level	*The ICT practitioners at this level manage certain parts of technical processes depending on their subject matter expertise. Many different profiles are served by professionals at this level who maybe fresh sub-degree graduates or those who possess certain experience in their field.*
Job Title	Information Security Technician
	Junior Information Security Analyst
	Junior Information Security Engineer
Support Level	*The ICT practitioners at this level provide basic technical support depending on their subject matter expertise. Many different profiles are served by the practitioners at this level who maybe S6 graduates with relevant ICT skills and knowledge or those who possess little experience in their field.*
Job Title	Computer Operator
	User Support Staff
	Technical Support Services Staff
	Help Desk Operator
	Field technician

Proposed Competency Requirements (Information Security - Master Level)

Relevant Job Titles:

- Chief information Security Officer / information Security Director

Area of Work / Cluster Name	Major Task	Competency Requirements	Units of Competency (UoCs) Number	Relevant Qualification for fulfilling Competency Requirements
organisational policies and strategies for information security	1. Provide the direction for the organization's data and information security protection, and oversee technology governance and policies	▪ Review and comply with organisational policies and procedures, relevant laws and regulatory requirements ▪ Review key controls metrics regularly to fulfill the security standard	111205L6 111166L6	Obtain qualification via training programmes (QF Level 6)
	2. Develop the organization's security strategy, security awareness programs, security architecture, and security incident response	▪ Establish corporate information security standards ▪ Develop information security standard, policies and guidelines for the company ▪ Develop an information system security audit plan ▪ Set policy to control data security and privacy	ITSWIS612A 111164L6 ITSWIS618A 111206L6	

Area of Work / Cluster Name	Major Task	Competency Requirements	Units of Competency (UoCs) Number	Relevant Qualification for fulfilling Competency Requirements
Risk Management for information security	3. Evaluate new information security threats and IT trends and develops effective security controls	▪ Review the emerging technologies and cross-functional strategies ▪ Design the evaluation criteria security test plans	111207L6 111168L6	(Continued) Obtain qualification via training programmes (QF Level 6)
	4. Provide strategic risk guidance for IT projects, including evaluation and recommendation of technical controls	▪ Review key controls metrics regularly to fulfil the security standard ▪ Devise processes for detecting, identifying and analyzing security incident	111166L6 ITSWIS613A	
	5. Collaborate with IT and other internal teams of the organization, and coordinate the IT component of both internal and external audits, to ensure security policies are in compliance with relevant laws and regulations	▪ Manage IT service management strategy ▪ Conduct security investigation	111204L6 ITSWOS619A	

Proposed Competency Requirements (Information Security - Specialist Level)

Relevant Job Titles:

- Information Security Architect / Information Security Engineer / Information Security Analyst / Cryptographer

Area of Work / Cluster Name	Major Task	Competency Requirements	Units of Competency (UoCs) Number	Relevant Qualification for fulfilling Competency Requirements
Identification of security threats	1. Keep up to date with the latest security and technology developments	▪ Compare the strengths and weaknesses of different cryptographic algorithms and determine the suitable algorithm for the company operation ▪ Appraise the security threats in emerging technologies ▪ Appraise Open-source intelligence (OSINT) methodology in the security process	111183L5 111182L5 111181L5	Obtain qualification via training programmes (QF Level 5)
	2. Monitor for attacks, intrusions and unusual, unauthorised or illegal activity	▪ Identify the potential security threats to the organisation ▪ Deliver security services for operations ▪ Ensure availability, integrity and confidentiality of information systems	111174L5 ITSWOS521A ITSWIS508A	

Area of Work / Cluster Name	Major Task	Competency Requirements	Units of Competency (UoCs) Number	Relevant Qualification for fulfilling Competency Requirements
Investigation and evaluation of security incidents	3. Research/evaluate emerging information security threats and ways to manage them. Test and evaluate security products	▪ Conduct investigation of Information Security Incidents ▪ Review the possible causes of the threats for remedial actions recommendation ▪ Evaluate and assess effectiveness of corporate information security practices	111169L5 111180L5 ITSWIS507A	(Continued) Obtain qualification via training programmes (QF Level 5)
	4. Identify potential weaknesses and implement measures, such as firewalls and encryption. Plan for disaster recovery and create contingency plans in the event of any security breaches	▪ Develop procedures to implement incident response plan ▪ Evaluate the results of application security assessment for improvement recommendation ▪ Perform network security assessment for the company ▪ Propose appropriate countermeasures to prevent security attacks	111170L5 111173L5 111176L5 111179L5	

Area of Work / Cluster Name	Major Task	Competency Requirements	Units of Competency (UoCs) Number	Relevant Qualification for fulfilling Competency Requirements
Investigation and evaluation of security incidents (Continued)	5. Maintain an information security risk register and assist with internal and external audits relating to information security	▪ Develop procedures to maintain and comply the information security standard and policies of the organisation ▪ Prepare and deliver information system security audit report ▪ Prepare documentation to report the security testing and findings ▪ Conduct operation security risk assessment and audit ▪ Enact information system security audit plan	111171L5 111177L5 111178L5 ITSWOS530A ITSWIS513A	(Continued) Obtain qualification via training programmes (QF Level 5)

Proposed Competency Requirements (Information Security - Practitioner Level)

Relevant Job Titles:

- Information Security Technician / Junior Information Security Analyst / Junior Information Security Engineer

Area of Work / Cluster Name	Major Task	Competency Requirements	Units of Competency (UoCs) Number	Relevant Qualification for fulfilling Competency Requirements
Implementation and maintenance of information security system	1. Assists with planning, implementation, and maintenance of the organization wide security systems	▪ Apply suitable network development tools in the deployment of secure network system	111190L4	Obtain qualification via training programmes (QF Level 4)
		▪ Support and implement information security practices and procedures	ITSWIS404A	
	2. Monitor system security access. Perform routine security tests and user account auditing	▪ Implementing monitoring equipment to monitor infrastructure failure and security breaches	111429L4	
		▪ Perform application security assessment for the organisation	111191L4	
		▪ Conduct drills according to response and recovery plans	ITSWIS406A	

Area of Work / Cluster Name	Major Task	Competency Requirements	Units of Competency (UoCs) Number	Relevant Qualification for fulfilling Competency Requirements
Implementation and maintenance of information security system (continued)	3. Respond to all reported security incidents and other reports of suspicious activity	▪ Maintain the security control documents ▪ Carry out the first line of communication for triggering client response and alert internal security teams ▪ Maintain security files by receiving, processing and filing the system data	ITSWOS418A 111192L4 111193L4	(Continued) Obtain qualifications via training programmes (QF Level 4)
Implementation of information security policies and guidelines for an organisation	4. Manages user accounts; assures defined user authentication procedures are strictly followed	▪ Ensure information security procedures and guidelines support information security policies ▪ Monitor and perform the system security access checking	ITSWIS402A 111194L3	

Proposed Competency Requirements (Information Security - Support Level)

Relevant Job Titles:

- Computer operator / User support staff / Technical support services staff (TSS) / Help desk operator / Field technician

Area of Work / Cluster Name	Major Task	Competency Requirements	Units of Competency (UoCs) Number	Relevant Qualification for fulfilling Competency Requirements
Network Support	1. Network Support	▪ Install and configure client/server application ▪ Configure WAN connection ▪ Troubleshoot network issues	107882L3 107883L3 107884L3	Obtain qualifications via training programmes (QF Level 3) Or RPL Mechanism (QF Level 3 RPL Cluster: TOS010L3)
Network Security Support (Technical Support)	2. Network Security Support	▪ Administer basic network security ▪ Administer basic website security ▪ Administer perimeter firewall ▪ Strengthen workstation protection	107887L3 107889L3 107890L3 107891L3	Obtain qualifications via training programmes (QF Level 3) Or RPL Mechanism (QF Level 3 RPL Cluster: ITOS011L3)
User Support	3. User Support	▪ Provide support to mobile device users ▪ Troubleshoot client device hardware issues ▪ Perform remote support	107904L3 107905L3 107907L3	Obtain qualifications via training programmes (QF Level 3) Or RPL Mechanism (QF Level 3 RPL Cluster: ITOS012L3)
System Security Support	4. System Security Support	▪ Create and maintain user accounts on server ▪ Configure user access control on server ▪ Administer system security	107885L2 107886L3 107888L3	Obtain qualifications via training programmes (QF Level 3) Or RPL Mechanism (QF Level 3 RPL Cluster: ITOS009L3)

Area of Work / Cluster Name	Major Task	Competency Requirements	Units of Competency (UoCs) Number	Relevant Qualification for fulfilling Competency Requirements
Web Support	5. Web Support	▪ Troubleshoot web browser and connection issues ▪ Maintain website performance ▪ Build simple web site using content management systems ▪ Maintain website	107909L3 107910L3 107911L3 107912L3	Obtain qualifications via training programmes (QF Level 3) Or RPL Mechanism (QF Level 3 RPL Cluster: ITOS013L3)
Network and Security Support	6. Network and Security Support	▪ Build a small wireless LAN ▪ Install and configure network components/devices ▪ Install and configure client/server application ▪ Strengthen workstation protection ▪ Troubleshoot web browser and connection issues	107879L2 107880L2 107882L3 107891L3 107909L3	Obtain qualifications via training programmes (QF Level 3) Or RPL Mechanism (QF Level 3 RPL Cluster: ITOS016L3)

Unit of Competency

Functional Area: Network Support

Title	Build a small wireless LAN
Code	107879L2
Range	This unit of competency applies to junior IT personnel who are involved with construction of the organisation's network infrastructure. The main duties include installing, configuring of small wireless local area network (LAN) as well as performing user training on the use of the wireless LAN. However, during the planning and network design and sourcing of equipment for the wireless LAN he/she may be required to provide advice and assistance.
Level	2
Credit	3
Competency	Performance Requirements 1. Knowledge to build a small wireless LAN: • Possess good communication and interpersonal skills • Possess good knowledge of basic training skills • Possess good knowledge of different network and wireless security risks • Possess good knowledge of wireless LAN components and their functions • Possess good knowledge of how to acquire technical manuals on wireless LAN equipment • Understand the network needs of users and the organisation • Possess good knowledge on use of network testing software 2. Building a small wireless LAN • Comprehend and assess the wireless LAN design diagram. Confirm and raise any concerns or suggestions with the designer or supervisor before purchase of equipment or install work. Area where he/she may assist include but not limited to the following: • Evaluate and/or selection of wireless equipment • Advice on any blind spots that affect the wireless signal • Site survey • Prepare for installation of wireless LAN • Identify the location of wireless router/Access Point and can be connected to the wired local network or to Internet service provider • Verify power availability for the wireless router • Verify Access Point (AP) has mounting space and signal are not obstructed that reduced transmission efficiency • Acquired network settings • All required equipment have been checked, verified working, and installation manuals are available • Install and configure the wireless router • Perform a wireless coverage test. Install wireless extension device to increase network coverage and remove blind spots, if needed • Configure security settings that conform to the network design and the organisation security policies • Install and configure wireless LAN cards on personal computers or join mobile client and smartphone to the wireless LAN then perform the following tests: • Test connection of the wireless network with user equipment to ensure general compatibility and access • Perform speed tests to ensure client connection is of expected performance • Perform security tests to ensure only authorised clients can connect to the wireless network • Label all wireless LAN equipment in accordance with the designed infrastructure plan/diagram • Provide instructions sessions and/or tutoring to users on use of wireless network, topics include: • Pairing with designated Service Set Identifier (SSID)

	• Logon arrangements • Use of wireless LAN equipment • Document all installation activities and record configuration and security settings details in accordance with the organisation’s guidelines and procedures 3. Exhibit professionalism • All installation activities and preparation of documents were performed in accordance with organisation guidelines and standards • Always protect the organisation against unauthorised wireless connection and apply industry network security best practices • Follow the organisation’s occupational health and safety guidelines and procedures when installing with network equipment
Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Perform the necessary preparations before the installation of wireless LAN • Install, configure and test the wireless LAN and equipment in accordance with the organisation’s requirements and standards • Provide sufficient and satisfactory training to users that enable them to access the organisation network resources
Remark	

Unit of Competency

Functional Area: Network Support

Title	Install and configure network components/devices
Code	107880L2
Range	This unit of competency applies to support personnel who install and configure network components or devices in a small internal Local Area Network (LAN) environment. A small network would comprise of Internet connection with wireless and wired Internetworking devices such as switches, routers, wireless LAN Access Points (AP).
Level	2
Credit	3
Competency	Performance Requirements 1. Knowledge for installing and configuring network components/devices: • Possess basic network troubleshooting skills • Possess good knowledge of system and network monitoring equipment • Possess good knowledge of internetworking devices • Possess good knowledge of network concepts, such as: • Network types • Types of cables and distance limits • Wireless LAN • Possess good knowledge of the TCP/IP protocol • Possess basic knowledge of procedures for handling electrical devices 2. Installing and configuring network components/devices • Comprehend the installation requirements including: • Types of network component/device • Verify location is suitable for the installation work • Prepare for installation work • Assess network component/device power and cabling needs • Verify location is suitable for the installation • Acquire the network component/device • Acquire technical manuals and comprehend the installation and configuration instructions • Acquire network configuration information for the network component/device • Perform the installation of network component/device complying to the organisation and manufacturer's procedures • Configure and test the network component/device to ensure it complies with the organisation's network requirement • Clean installation site and return equipment to appropriate location • Document the installation and configuration according to the organisation guidelines and standards 3. Exhibit professionalism • Adhere to the organsiation's occupational safety procedure • Well converse with industry's networking best practices
Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Be well prepared for the installation work • Follow the work order and install the network component/device according to the manufacturer and the organisation procedures • Perform post installation procedures satisfactorily and well document the configuration details and installation work according to the organisation standard procedures
Remark	

Unit of Competency

Functional Area: Network Support

Title	Install and configure client/server application
Code	107882L3
Range	This unit of competency applies to support personnel who install and configure client/server application at workplace. The installation may be for a fresh deployment of the organisation wide client/server application or re-installation when client/server application is having issues. The type of client/server application this UoC refers to is of “tightly coupled” type like POS (Point Of Sales) systems rather than “loosely coupled” type like web browser to web server (any). Also it is installed in an internal network.
Level	3
Credit	6
Competency	Performance Requirements 1. Knowledge for installing and configuring client/server application • Possess basic literacy skills to comprehend work orders and technical documents • Possess basic knowledge of networking concept • Possess good knowledge of client and server concept in particular • Possess good knowledge of common operating systems (server and client) • Possess good knowledge of testing and troubleshooting client/server applications 2. Install and configure client/server application • Develop installation plan for the client/server application requirements including but not limited to the following: • Identify what installation options are required from work order • Identify hardware requirement (i.e. server and client side) • Identify software requirement (i.e. database, middle ware, etc.) • Identify network requirements • Identify security requirements • Identify what data migration is required, if any • Preparing for installation • Upgrade hardware of server and client device, if required • Acquire the client/server application installation media • Familiarised with the client/server application installation instructions from vendor documents • Acquire associated settings for the client/server application, such as: • IP address of the server and client • Network settings • Authorised access account settings • Acquire all necessary technical manuals • Backup the server and client systems • Install and configure network protocol, middleware, database, if required • Install and configure the server side of the client/server application as required by the work order • Configure security and access settings to allow client to connect • Undertake restore or migration of data, if required • Perform appropriate tests • Install and configure client side of the client/server application as required by the work order • Configure security setting to enable access to the server side • Configure appropriate functions of the application • Perform tests to ensure client side is forming as required • Perform post installation procedures • Clean up work area and remove temporary work files and objects from the server and client device

	• Perform backup image of the server and client for system restore, when and if required • Return and store installation media in secure place as instructed by the organisation’s guideline • Document the installation and configuration according to the organisation guidelines and standards 3. Exhibit professionalism • Adhere to the organisation’s occupational safety procedure • Well converse with industry’s best work practices for installing client/server applications
Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Perform the pre-installation activities and being well prepared to ensure the installation of the client/server application without any delay • Ensure the installation process was carried out efficiently without affecting other applications and/or services on the server and clients side • Perform post installation procedures that complied with the organisation guidelines and procedures
Remark	

Unit of Competency

Functional Area: Network Support

Title	Configure WAN connection
Code	107883L3
Range	This unit of competency applies to IT support personnel who are responsible to configure the organisation’s internal network to connect and communicate with the external Wide Area Network (WAN) or be connected to the Internet. The configuration will involve configuring the organisation’s routers as well of internal hosts. Hosts in this UoC can be user client devices (PCs, mobile devices, tablets, wireless APs, etc.) or servers.
Level	3
Credit	3
Competency	Performance Requirements 1. Knowledge for configuring WAN connection: • Possess good literacy skills to interpret network diagram/plan, technical documents, equipment manuals and specifications • Possess basic network installation and configuration skills • Possess good knowledge of internetworking devices • Possess detailed knowledge of the TCP/IP protocol • Possess good problem solving skill • Possess basic knowledge of organisation guideline and safety procedures for handling electrical devices 2. Configure WAN connection • Prepare the readiness of the internal network to connect with the WAN, including the following: • Comprehend the organisation network plan and architecture, including: • Number of internal subnets • Routing settings of each subnet • De-Militarised Zone (DMZ) information • Load balancing for multi WAN connections • Acquire and install router as per required by manufacturer • Acquire internal network settings from network administrator and configure into the router • Liaise with WAN service provider to confirm switch-over date and WAN connection to be installed • Determine connection type (static IP or DHCP assigned) and configure with reference to the organisation’s network plan. For static IP address connection to the WAN, acquire the network setting from service provider • Configure and test router with the given WAN IP address • Test the internal and external connection to ensure traffic can flow on both directions • Configure and test host connections • Document the installation and configuration details according to the organisation guideline and standards 3. Exhibit professionalism • Adhere to the organisation’s occupational safety procedure • Well converse with industry’s networking best practices

Unit of Competency

Functional Area: Network Support

Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Liaise with WAN service providers to coordinate the cabling and installation of WAN modems into the premises that conform to the network diagram/plan • Configure and test router connection with the WAN connection • Configure all hosts of the internal network to enable them to communicate via the WAN connection
Remark	

Unit of Competency

Functional Area: Network Support

Title	Troubleshoot network issues
Code	107884L3
Range	This unit of competency applies to junior IT personnel who are involved with troubleshooting network issues while in a network supporting role. These junior IT personnel is expected to troubleshoot operational wireless and wired network problems, such as device connection issues, software configuration issues, and network component failure issues. For this UoC devices could be: personal computers, notebooks, tablets, smartphones, internetworking components such as routers, switches, etc.
Level	3
Credit	3
Competency	Performance Requirements 1. Knowledge to troubleshoot network issues: • Possess good communication and interpersonal skills • Possess good network troubleshooting skills • Possess basic knowledge of different network technologies • Have good understanding of network components and their functions • Possess good knowledge of how to acquire technical information from manuals, colleagues and Internet • Possess good knowledge in operating network testing equipment

Unit of Competency

Functional Area: Network Support

<table>
<tr><td>Competency</td><td>2. Troubleshooting network issues
<ul>
<li>Acquire details of network issues from problem reports or by communicating with users to understand symptoms of network issues</li>
<li>Attempt to reproduce the network issues on user’s client device or network component, if possible</li>
<li>For wired network connection issues
<ul>
<li>Inspect for loose cabling on the network devices, network clients, and network components. Reconnect and secure cables</li>
<li>Use cable testing equipment to test cable to ensure it is still functioning</li>
</ul></li>
<li>For wireless connection issues
<ul>
<li>Determine where the issues lie, at wireless client or Access Point side
<ul>
<li>Verify the wireless access point is functioning using other devices or clients</li>
<li>Verify the wireless connection setting and the correct password is used at the client side</li>
</ul></li>
</ul></li>
<li>For software configuration issues
<ul>
<li>Acquire network settings from network administrator</li>
<li>Verify the software configuration setting matched the network settings. Reconfigure if necessary</li>
</ul></li>
<li>For network component issues
<ul>
<li>Verify the device is receiving power
<ul>
<li>Perform visual check if power cable is connected</li>
<li>Verify power adapter of the device is working and securely connected</li>
<li>Verify the device’s power is on</li>
</ul></li>
<li>Verify the device configuration setting is correct</li>
<li>Verify the device is transmitting and receiving signals</li>
</ul></li>
<li>Document all troubleshooting activities and record all findings. Also complete problem report in accordance with the organisation’s guidelines and procedures</li>
</ul>
3. Exhibit professionalism
<ul>
<li>All troubleshooting activities and preparation of documents were performed in accordance with organisation guidelines and standards</li>
<li>Follow the organisation’s occupational health and safety guidelines and procedures when working with network equipment</li>
</ul></td></tr>
<tr><td>Assessment Criteria</td><td>The integrated outcome requirements of this UoC are the abilities to:
<ul>
<li>Prepare sufficiently for the troubleshooting job</li>
<li>Systematically perform troubleshoot tasks and find the network issues</li>
<li>Follow procedures and be able to prepare documents and complete problem reporting in accordance with organisation standard</li>
</ul></td></tr>
<tr><td>Remark</td><td></td></tr>
</table>

Unit of Competency

Functional Area: Security Support

Title	Create and maintain user accounts on server
Code	107885L2
Range	This unit of competency applies to support personnel who administer the organisation's servers. A very important task for the administrator or the support personnel of servers is to create accounts of users that are allowed to access the system's resource. This UoC assumes servers are standalone and not in directory service environment
Level	2
Credit	3
Competency	Performance Requirements 1. Knowledge for creating and maintaining user accounts on server • Possess system troubleshooting skills • Possess good knowledge of system logs • Possess good knowledge of common server operating systems • Possess good knowledge of operating system's access control • Possess basic knowledge of information security • Possess knowledge of the organisation's user security procedures and guidelines

Unit of Competency

Functional Area: Security Support

Competency	2. Create and maintain user accounts on server • Determine the needs of the accounts on server, such as: • The role of the user (user, administrator, operator, etc.) • Which server, if there are more than one • Personal folder for the user • Access to server resources • Application settings • Access rights • Login to server with administrative account to create the new account and follow the organisation guidelines to setup security settings for the account based on the role of the user. Settings include but not limited to the following: • Security role of the account • Directory and file permissions • Password length • Change password requirements and duration • Set temporary password and set user must-change-password on first login • Inform the user of new account details • Regularly use system tools or third party tools to determine security and usage of accounts, such as but not limited to the following: • Accounts involved with unusual activities • Attempt to access unauthorised resources • Accounts locked out • Unused accounts • Handle unusual account activities in accordance to the organisation guideline, such as escalating to supervisor • Verify unused accounts and follow the organisation procedures to perform clean-up activities, such as remove account, revoke permission, etc. • Document and record all actions performed on user account in accordance with the organisation guidelines 3. Exhibit professionalism • Apply system administrator ethics and exercise due diligence when administering user accounts on servers • Exhibit security attitude but balance the needs of users with the organisation security needs when administering system user accounts, as well as securing the server
Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Understand the needs for creating new accounts • Use appropriate system tools to create accounts, perform correct configurations, setup correct access rights to server resources and provide sufficient details and guidance to user that enabling him/her to access the server • Monitor account usage and account irregular activities and take corrective actions to maintain accounts current and secured on the server
Remark	

Unit of Competency

Functional Area: Security Support

Title	Configure user access control on server
Code	107886L3
Range	This unit of competency applies to support personnel who administer the organisation’s servers. To access resources on a server the user will need appropriate access rights which administrator will need to configure. Access control in modern servers has pre-configured access control in form of different roles or via traditional access rights.
Level	3
Credit	3
Competency	Performance Requirements 1. Knowledge for configuring user access control on server • Possess system troubleshooting skills • Possess good knowledge of system logs • Possess good knowledge of common server operating systems • Possess good knowledge of operating system’s access control • Possess basic knowledge of information security • Possess knowledge of the organisation’s user security procedures and guidelines 2. Configure user access control on server • Determine what role the user is allocated by the organisation, for example: • Administrator • Backup operator • Application administrator • Read only analyst • Use server management tools to assign the role to the user’s account • Determine resource access permitted for the user, such as but not limited to the following: • Local logon • Internet access • Remote logon • Use server tool to configure user accounts with allowed access • Create a check list of access control setting for each shared resources and/or object, such as but not limited to the following: • Printers • Folders • Files • Applications • Configure the allowed access and level of access (Read, Write, Execute, etc.) to each object and shared resource • Document and record all user access setting and configuration for reference 3. Exhibit professionalism • Comply system administrator ethics and exercise due diligence when administering user accounts and access control on servers • Exhibit security attitude but balance the needs of users with the organisation security needs when setting user access control as well as protecting the server

Unit of Competency

Functional Area: Security Support

Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Determine and setup the role of the user that matches his/her access on the server • Identify all the individual objects, shared resources on the server which the user requires access to • Setup and configure correctly the user's access control on the server
Remark	

Unit of Competency

Functional Area: Security Support

Title	Administer basic network security
Code	107887L3
Range	This unit of competency applies to support personnel who administer the organisation’s network security on their regular day to day duties. The duties include supporting users request for network access and ensuring the network is protected in accordance with the organisation’s requirements. The organisation network infrastructure, in this context, is a small or simple type which may consists of one perimeter firewall, WAN Internet router, wireless LAN Access Point (AP) for mobile clients, one central switch and a number of group switches with hosts (workstations or servers) connected. Network services may include: file service, network printing, Virtual Private Network (VPN) or remote access, etc.
Level	3
Credit	3
Competency	Performance Requirements 1.Knowledge for administering basic network security: • Possess good communication and interpersonal skills • Possess network troubleshooting skills • Understand system and network monitoring equipment logs • Able to operate the organisation network devices • Possess broad knowledge network function and features of network devices • Possess knowledge of threats and the importance of network security • Possess knowledge of the organisation’s network security procedures and guidelines

Unit of Competency

Functional Area: Security Support

Competency	2. Administer basic network security • Comprehend the organisation’s network infrastructure, daily activities list and security policies • Determine the network security status including but not limited to the following: • Network devices are operating normally via visual check, including: power lights are on, cables are not loose • Review monitoring and system logs and audit reports to ensure no unauthorised access or irregularities • Ensure Internet security (antivirus, anti-spyware) filtering/detection systems are still effective and up to date • When irregularities are detected, analyse, evaluate and handle irregularities in accordance with the organisation’s procedures, seek assistance if necessary. Actions may include: • Adjust firewall rules, • Change wireless AP security passwords. • Segregate guest mobile users, if necessary • Train users on network security functions • Adjust access control on network resources • Report irregularities to supervisor • Facilitate user’s request to define and configure suitable level of network access on network controlling devices but ensure it conformed to the organisation security specifications • Regularly perform security patches and updates of network devices when required • Regularly review and evaluate the network security to ensure it is well protected and conforms to the organisation needs and complied with regulatory requirement, if any • Document actions/changes to the network in accordance with the organisation’s procedures. Consult with colleagues and supervisors when required 3. Exhibit professionalism • Ensure network security complied with the organisation and regulatory requirements • Exhibit security attitude but balancing the need of users with the security need when administering the network security • Well converse with industry network security best practices and keep updated with trends of network security
Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Analyse security logs and reports to determine security irregularities • Handle and rectify network security irregularities in accordance with the organisation procedures • Set the correct level of network access for users in accordance with the organisation procedure
Remark	

Unit of Competency

Functional Area: Security Support

Title	Administer system security
Code	107888L3
Range	This unit of competency applies to support personnel who administer the organisation’s system security on client devices. The duties of support personnel includes installing various security applications, performing various system configuration and setting to protect the system from loss of information (user and organisation) and different network security risks. Client devices mainly refer to personal computers, notebooks and business tablets
Level	3
Credit	3
Competency	Performance Requirements 1. Knowledge for administering system security • Possess good communication and interpersonal skills • Possess system troubleshooting skills • Possess good knowledge of system and network logs • Possess good knowledge of common operating systems • Possess broad knowledge on functions and features of network devices • Understand network security and system security risks • Possess knowledge of the organisation’s security procedures and guidelines 2. Administer system security • Comprehend the organisation’s system security requirements and system security plan, including but not limited to the following: • List of authorised personnel/users that can access the system • Level of access/tiered access, or what each user is allowed and not allowed to do on the system • Access control methods, or how users will access the system (user ID/password, digital card, biometrics) • System setting and application needed to strengthen the system and how weaknesses are handled • Which system required system backup and what type of backup procedure to apply • Network security settings and configurations • Install the required security application, such as: • Antivirus and spyware protection applications • Personal firewall • Malware protect application • Configure and set remote access and support function according to the organisation guideline and procedure • Configure network and firewal • according to the organisation’s guideline • Create and setup user accounts in accordance with organisation security requirements • Review files security settings and modify access and read/write permissions to match user’s role. • Regularly perform backups, system security checks, system updates • Monitor and record security checks • Document and record details of installed applications, configurations, settings, risks for system audit, maintenance and support purpose 3. Exhibit professionalism • Exhibit security attitude but balance the need of users with the organisation security need when administering system security

Unit of Competency

Functional Area: Security Support

Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Comprehend the system security plan • Install the required security applications, correctly configure and perform appropriate setting that complied with the security plan • Perform scheduled system security checks, system update and document system changes in accordance with the organisation's guidelines and procedures
Remark	

Unit of Competency

Functional Area: Security Support

Title	Administer basic website security
Code	107889L3
Range	This unit of competency applies to support personnel who are responsible to administer security of the organisation’s website under the direction of supervisor. The server on which the website resides on, either locally or remote hosted should be protected from hackers, virus, unauthorised access, hijacked. Monitor and validate the web page, scripts, SQL commands used does not have vulnerabilities for malicious attacks which can affect the organisation’s network or systems or theft of the organisation’s business data.
Level	3
Credit	6
Competency	Performance Requirements 1. Knowledge for administer basic website security • Knowledge of different website security risks and the importance of website security protection • Understand the use of website security audit tools • Possess a broad knowledge of server and network security • Possess good knowledge of the organisation’s security requirements and policies • Possess good knowledge of website protection technologies and trends • Possess good knowledge of installing and configuring hardware and software 2. Administer basic website security • Work with the supervisor to identify the security needs of the organisation’s website, including but not limited to the following: • Website functionality • Access requirement of transactions, visitors and users • Operating Systems weaknesses • Secure the server of the website with installation of site certificate, regular system patches and updates, antivirus, anti-spyware protection and updates • Configure web server securely with required functionality and features only • Secure website transactions with encryptions • Set access control of server and database to those needed access only • Work with website content development team to ensure scripts and web applications are vulnerabilities free • Regularly use monitoring and audit tools to test and monitor vulnerabilities of the website • Perform regular offline backup of the website • Continue to develop or help to secure procedure to secure the organisation’s website that comply with the organisation security requirements 3. Exhibit professionalism • Committed to protect the organisation’s assets • Exhibit security attitude but balance the business needs against the security need when administering the website security • Well versed with industry network security best practices
Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Secure the organisation’s website that complied with the organisation’s requirement • Use audit and monitoring tools to reduce the website vulnerabilities • Set the correct level of network access for users in accordance with the organisation procedure
Remark	

Unit of Competency

Functional Area: Security Support

Title	Administer perimeter firewall
Code	107890L3
Range	This unit of competency applies to IT personnel who administer the organisation’s network security; particularly the perimeter firewall which protects the organisaton internal network from the external network. The administering tasks of these IT personnel include but not limited to: maintain firewall filtering rules, monitor security logs, perform maintenance of the firewall, ensure the firewall is always on, etc.
Level	3
Credit	3
Competency	Performance Requirements 1. Knowledge for administering perimeter firewall: • Possess good communication and interpersonal skills • Possess detailed knowledge of network security and different risks • Possess detailed knowledge of firewall concept • Possess good knowledge of operating firewall and monitoring equipment • Understand the organisation’s network security requirements and policies • Well updated with network security threats, technologies and trends 2. Administer perimeter firewall • Perform regular monitoring of perimeter firewall to ensure it is fully functioning. • Perform reconfiguration of settings when required. Configuration settings that affect security of the network must follow the organisation guideline and procedures before action • Manage firewall filtering rules to match the organisation’s and process users needs, including: • Create new rules • Amend existing rules • Remove redundant and conflicted rules • Regularly review the list of filtration rules to verify rules still effective and are being used. Cleanup unused rules to maintain efficiency and performance of the firewall • Regularly monitor and review access logs to ensure no security breach or any irregularities. When irregularities found, escalate to supervisor and investigate • Assist supervisor to review operation procedures, such as “filtration rule change” requests • Perform backup of firewall database after any change of settings or filtering rules • Document all changes (configuration, rules) and actions performed on the firewall in accordance to the organisation standards 3. Exhibit professionalism • Ensure perimeter protection complied with the organisation guideline • Exhibit security attitude but balancing the need of users with the security need when administering the perimeter security • Well converse with industry network security best practices
Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Set up the firewall that matches the organisation business requirements and securely protect the internal network from external environment • Use the firewall monitoring facilities or security log to monitor irregular activities • Follow the orgnaisation’s procedures to document all changes and actions made on the firewall
Remark	

Unit of Competency

Functional Area: Security Support

Title	Strengthen workstation protection
Code	107891L3
Range	This unit of competency applies to support personnel who are responsible for securing client workstation. Workstations are vulnerable to local and external threats, they need to be protected from as much as these threats as possible. Most organisation will have different protection procedures which support personnel need to setup before allowing user to access the workstation. This UoC illustrates some of the protection tasks and it is by no means exhaustive.
Level	3
Credit	3
Competency	Performance Requirements 1. Knowledge for strengthening workstation protection • Possess system troubleshooting skills • Possess detailed knowledge of security features and functions of the organisation’s operating systems • Possess good knowledge of system security concepts • Possess good knowledge of computer hardware and system software • Possess knowledge of the organisation’s security procedures and guidelines

Unit of Competency

Functional Area: Security Support

Competency	2. Strengthen workstation protection • Comprehend the organisation's guideline for workstations protection to configure the user's workstation. Systematically setup and configure protection features on the workstation • Setup physical security protection, including but not limited to the following: • Lock the CPU unit to prevent opening of the case • Affix a chain lock (Kensington lock) to secure position for notebooks • Setup password protection (hardware-level) for access to machine's BIOS • Eliminate or disable unnecessary services. For example: remote access, Internet sharing, etc. • Remove unnecessary executables and registry entries to prevent attacker invoking disabled programs • Set user account to • "non-administrator" account, to prevent uncontrolled change of system settings • Avoid multi-user sharing same machine, if possible • Set system account policies • Minimum length of account password • Force change password • Set re-used policy • Setup screen save to turn off screen and power off system after a predefined period of no user activities • For systems holding confidential information, setup file encryption and access permission • Install and setup anti-virus, anti-spyware and anti-malware scanning and handling, such as: • Auto and scheduled update of virus definitions • Scheduled daily scan • Real time protection • Anti-virus application which starts on system boot • When virus or malware found, clean first (high risk) and quarantine second • Setup firewall protections • Setup auto and scheduled system updates • Create a backup image of the workstation before allowing user to use the machine • Document the system settings and configurations for internal record 3. Exhibit professionalism • Exhibit security ethics and balance the need of users with the organisation security needs when setting and configuring security protection of user's workstations
Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Comprehend the organisation's workstation protection guidelines and able to configure and setup required security protections • Complete documents of the security settings and configuration in accordance with the organisation's procedures
Remark	

Unit of Competency

Functional Area: System and Hardware Support

Title	Provide support to mobile device users
Code	107904L3
Range	This unit of competency applies to IT support personnel who are responsible for mobile device support to users. As organisations are joining the Bring Your Own Device (BYOD) bandwagon, users will need supporting in the work environment; IT support staff will need to have the necessary skills to support and educate users using mobile devices to access the organisation resources. This UoC concerned on area of general support including but not limited to: setup brand new devices to access organisation resources, assist logon and use of Mobile Device Management (MDM) system, protection of corporate information in event of loss of mobile devices, remote support access and support, change configuration and settings, etc.
Level	3
Credit	6
Competency	Performance Requirements 1. Knowledge to perform remote support: • Possess good communication, listening and interpersonal skills • Possess remote support skills capable to perform troubleshooting, provide instructions systematically and remote problem solving • Possess good knowledge of functions and features of the organisation's MDM system • Possess good knowledge of mobile device supported applications • Possess good knowledge of common mobile device platforms such as IOS, Android, Blackberry, Windows Phone, etc. • Well conversed with the organisation's BYOD guidelines and procedures • Possess good knowledge of virtual desktop technology and Virtual Desktop Infrastructure (VDI) for mobile device

Unit of Competency

Functional Area: System and Hardware Support

Competency	2. Perform remote support • Listen attentively and patiently to understand the user’s reported issues • Refer to the Trouble Ticket System (TTS)/problem reporting system to determine if similar issues and/or solutions exist • For brand new BYOD mobile devices, follow the organisation guidelines to perform some but not limited to the following tasks: • Ensure user understand, agree and accept the organisation policies, particularly when device is misplaced/lost • Install organisation MDM apps and organisation’s standard apps • Install mobile support apps, such as: Teamviewer for mobile, Remoty, GotoAssist, etc. • Configure network access setting such as VPN • Backup device • Turn on remote wipe function of the device • Install anti-virus/malware/spyware app • Create new access accounts on MDM server and test connectivity and accessibility to ensure device is function as expected • For troubleshooting or remote support, mobile support application or MDM apps should be used to remote access to the mobile device, to view and change setting, screen capture, direct communicating with user to provide instructions to resolve the issue • For misplaced/lost device, evaluate the risk of data loss and assist the user to use “find my phone/device/mobile” function or use MDM apps to trace, lock or wipe the device • Provide instructions and/or training to users on mobile devices usage and mobile security to protect organisation data • Create a new or update Trouble Ticket (TT)/problem report to record the activities transacted during the support session 3. Exhibit professionalism • Possess customer service oriented attitude • Apply industry best practices for mobile support and being up-to-date with mobile technology trends
Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Set up the users’ mobile devices to conform with the organisation’s mobile device policies • Use appropriate tools to troubleshoot mobile devices, resolve users experience issues and assist or advice users with correct solutions to resolve issues for providing effective support to users and protect the organisation data in the event of user loss • Take correct actions to protect the organsiation’s data in the event where users have lost mobile devices • Provide sufficient instruction or training to users on use of mobile devices that conform with the organisation policy
Remark	

Unit of Competency

Functional Area: System and Hardware Support

Title	Troubleshoot client device hardware issues
Code	107905L3
Range	This unit of competency applies to IT support personnel who are responsible for providing support for client devices. Client devices ranging from personal computer to smart mobile device could experience hardware issues during its operation and support personnel are requested to fix the issues. This UoC concerns the identification of hardware issues before it can be fixed.
Level	3
Credit	3
Competency	Performance Requirements 1. Knowledge for troubleshooting client device hardware issues • Possess good troubleshooting and problem analysis skills • Possess good knowledge of operating client devices • Possess good literacy skills for reading technical manuals of client devices • Possess good knowledge of the organisation's procedures for troubleshooting client devices • Possess basic knowledge of hardware protection procedures, such as use anti-static straps, etc. • Possess basic knowledge of the organisation health and safety guideline 2. Troubleshoot client device hardware issues • Comprehend symptoms, if any, prior issues appeared from problem report and/or discussion with user. For example: • Nothing came on when power button pressed • Blank screen but CPU unit appears to be running • System running very slow and continuously rebooting or hanged • System not responding to mouse and keyboard • Review maintenance records of the device, to determine if maintenance work has contributed or caused the issues • Prepare for troubleshooting: • Acquire all necessary technical and user manuals • Acquire tools to open the client device and tools for troubleshooting • Acquire device components or spare parts • Analyse and formulate a troubleshooting plan • Without opening to inspect the inside of the client device, perform checks for loose connections, power sockets, battery, display device, etc. • View the BIOS error message display code or listen for the number beeps sounded and verify the given code with technical manuals to identify BIOS detected error. For example: • 1 = Loose memory module • 2 = CPU error repair/replace mother board • 3 = display memory error repair/replace display card • Next stage of checking is to verify connected components have not affected the functioning of client device, such as: • Keyboards/mouse (swap with a known working component) • Battery low power on mobile device (swap with a fully charged battery) • Hard disk failure (listen for unusual noise) • Power supply unit failure (verify cooling fan is functioning and/or system light is on) • For intermittent issues, such as "system hang" or "randomly rebooting" under heavy system work load, identify cause of issue using combination of techniques, including but not limited to the following: • System log messages • Reproduce the issues with monitoring tools • Incorrect BIOS settings

	• Overheating components • Purpose-built hardware analysis device • For mobile device, once verified it is not battery problem and still cannot be started, return the devices to vendor who will use manufacture’s hardware problem analysis devices to identify the issues • Once the cause of issues have been identified, formulate a rectification action plan and clean the work area • Document and record the findings in accordance with the organisation procedures and standards 3. Exhibit professionalism • Follow organisation safety guidelines and procedures when performing troubleshooting of client devices
Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Prepare well with troubleshooting work, having all the required tools and manuals for use during the troubleshooting process • Plan the troubleshoot work and systematically perform the troubleshooting to identify the issues or cause of issues • Follow the organisation safety procedures during the troubleshooting process
Remark	

Unit of Competency

Functional Area: System and Hardware Support

Title	Perform remote support
Code	107907L3
Range	This unit of competency applies to support personnel who are responsible for providing remote support. In a structure support team this would be a Level 2 support personnel where Level 2 is normally the first point of escalation, provides guidance and instructions to Level 1. Level2 is where the support personnel take ownership of incidents where subject matter expertise and experience is required for diagnosis. However, this UoC concerned only remote support competencies and does not distinguish the organization level.
Level	3
Credit	3
Competency	Performance Requirements 1. Knowledge to perform remote support: • Possess good communication and interpersonal skills • Possess remote support skills capable of performing troubleshooting and providing systematic instructions for remote problem solving • Possess good knowledge and operating remote support applications • Understand committed Service Level Agreement (SLA) and standards • Possess good knowledge of problem escalation procedures and guidelines • Possess basic knowledge of the organisation computer hardware, Operating System (OS), applications and network equipment

Unit of Competency

Functional Area: System and Hardware Support

Competency	2. Performing remote support • Comprehend reported problem from Trouble Ticket system (TTS)/problem report system to understand symptoms and diagnostics from support desk colleague (level 1 support) • Search TTS/problem report system to determine if similar issues and/or solutions exist • Communicate with the customers/users to explain actions that will be performed to resolve the issue, such as: • Need to collect more information related to the reported issue • Need to remote access to user's system • Will instruct the user to self-rectify the issue upon determination that the user is capable of self-rectification • If remote access/control is necessary, determine customer/user's comfort level to have remote access feature of the system turn on and installation of remote access software. To gain customer/user's support it is necessary to explain: • How the remote access work compare with on-premise support • There are no security risks • Benefits of remote access/control • Perform troubleshoot and/or apply solution to correct the reported issue. If remote solution cannot fix the issue then offer to customer/user the on-premise support option • Confirm solution is acceptable with customer/user • Uninstall any application and/or reset configurations that were used for the remote support purpose and remind users to set off remote support functions on their system • Document all activities and record changed setting in the TTS/problem report. Where necessary, coordinate with other colleagues, such as requesting on-premise engineers to visit the customers/users 3. Exhibit professionalism • Possess customer service oriented attitude • Always keep customer informed of actions and status of the rectification process • Follow industry best practices to use best remote support application to provide remote support
Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Comprehend the reported problem from the internal TTS/problem report system and able to update the appropriate record in accordance with the organisation's procedures after the completion of the remote support session • Persuade customers/users to allow remote access/control to their system for troubleshooting and/or correcting of issues • Perform the remote support to the satisfaction of customers/users
Remark	

Unit of Competency

Functional Area: Web Support

Title	Troubleshoot web browser and connection issues
Code	107909L3
Range	This unit of competency applies to support personnel who are responsible for providing front line support on web browser usage to users on different client platforms, including desktops, notebooks, tablets and even smartphones. The web browser is one of the most used applications. Very often users will encounter many issues which will need assistance. Common issues encountered including but not limited to the following: cannot start browser, wrong security setting, incompatibility, malware, connection problem, unable to initiate download after click of links, etc. To assist users the support personnel will troubleshoot and provide a remedy. Additionally the support personnel should provide some basic tutorial to users to avoid repetition and facilitate self-help.
Level	3
Credit	3
Competency	Performance Requirements 1. Knowledge for troubleshooting web browser and connection issues: • Possess good communication and interpersonal skills • Possess good troubleshooting skills and capable of providing systematic instructions for remote problem solving • Possess good knowledge of functions of various web browsers on different platforms • Possess basic knowledge of operating different computing platforms • Possess basic knowledge of web browser development and trends such as: technologies, web browser features, malwares attacks, etc. • Possess basic knowledge of the organisation’s network infrastructure

Unit of Competency

Functional Area: Web Support

Competency	2. Troubleshoot web browser and connection issues • Patiently listen to user describing issues and symptoms. Use appropriate questioning techniques to gather as much information to help troubleshoot the issue: • What are the types of issue user is experiencing, • What type of browser • What platform and OS environment the browser is operating on • Refer to history problem log to determine if similar problems and solutions exist • If web browser shows “cannot connect to server” or similar message, then troubleshoot network connection by verifying and correcting below items: • Verify the client is actually connected to the network (LAN or mobile) • Verify client has acquired a valid IP and DNS address • Verify correct proxy server setting • etc. • If displayed content is inconsistent with the new contents of the web site, then clear the cache of the browser • If downloads are not permitted or no activities after user clicked a link, then review and adjust the security settings that prevent certain risky functions and scripts from auto activated, such as: ActiveX, cookies and downloads. Any adjustment of security setting must be complied with the organisation security policies • If web browser cannot start then locate related error messages from system or application logs to determine the issue. If application is corrupted, and no alternative method of correcting the problem, then uninstall and reinstall the Web browser • If the browser consistently redirected to unwanted web site, this may be due to the browser being hijacked by malware. Use anti-malware software to detect and remove the malware • Explain the cause of issues and remedies applied to users and provide some basic training and advice to user on “best practices on using web browser and surfing internet” • Create or update problem log in accordance with the organisation’s procedures and issues and remedies performed 3. Exhibit professionalism • Possess customer service attitude with desire to assist users with problems • Follow organisation safety guidelines and procedures when troubleshooting and/or reification of equipment
Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Systematically apply web browser troubleshooting techniques to identify the cause of issues and provide remedies • Use correct level of technical language to gather information related to the Web browser issues and conduct tutorial to users • Complete the “after event” procedures in accordance with the organisation’s standards
Remark	

Unit of Competency

Functional Area: Web Support

Title	Maintain website performance
Code	107910L3
Range	This unit of competency applies to IT support personnel who are responsible to maintain the performance of the organisation's website. One of the tasks of website maintenance is to ensure the site is running at an optimal speed that can provide a good user experience to visitors and a successful website with business.
Level	3
Credit	3
Competency	Performance Requirements 1. Knowledge for Maintain website performance • Possess good knowledge of various website performance testing tools, such as : Webpage analyser, Google's site tool and Google Page Speed, Yahoo's YSlow, etc. • Possess good knowledge of creating web contents • Possess basic knowledge of different web browsers • Possess good knowledge of the organisation basic network infrastructure • Possess good knowledge of the organisation website performance requirements 2. Maintain website performance • Work with supervisor and/or colleagues to identify the website response time required. Different types of responses for different types of contents • Verify the website performance using suitable performance testing/measuring tools • Study the website network and hosting server performance • If loading is high, consider off load some of the tasks from the server • If web server is hosted on a Cloud Server, consider using a different hosting service provider • Work with content developers to review and advice on some but not limited to the following: • Minimise size of webpage • Minimise the use of nested table • Avoid using oversized image file straight from camera. Resize image files to a match the purpose • Optimise programs, scripts and databases • Regularly run stress tests to ensure the performance of the website is within the organisation's standard • Document performance test results for reporting purpose 3. Exhibit professionalism • Possess quality of service attitude. Website performance affects the organisation image and business
Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Work with supervisors or colleagues to identify the and formulate a performance standard for the organisation's website • Use performance measuring tools to determine the performance of the organisation website • Work with website developers to improve performance of the website to meet the organisation's performance requirement
Remark	

Unit of Competency

Functional Area: Web Support

<table>
<tr><td>Title</td><td>Build simple web site using content management systems</td></tr>
<tr><td>Code</td><td>107911L3</td></tr>
<tr><td>Range</td><td>This unit of competency applies to IT personnel who are responsible for building a simple web site for the organisation. Most companies will want to have an Internet presence; having at least a simple web site and IT personnel are entrusted with building this web site. As Internet and web content management system (CMS) technologies are maturing, building web sites is almost as simple as creating “Office” documents. However, once the web site is built the IT personnel will need to provide tutorials to webpage designer on use of CMS editor to build webpages. This UoC assumes the web site is hosted by hosting service provider.</td></tr>
<tr><td>Level</td><td>3</td></tr>
<tr><td>Credit</td><td>3</td></tr>
<tr><td>Competency</td><td>Performance Requirements
1. Knowledge for building simple web site using content management systems
<ul>
<li>Possess good communication and interpersonal skills</li>
<li>Possess good knowledge of web hosting concept and sourcing of hosting facilities</li>
<li>Possess detail knowledge of implementing web CMS systems</li>
<li>Possess detail knowledge of operating and administering the organisation’s CMS</li>
<li>Possess basic knowledge of HTML</li>
<li>Possess some basic training skills</li>
</ul>
2. Build simple web site using content management systems
<ul>
<li>Work with supervisor and other stakeholders to identify the website technical requirements from, such as:
<ul>
<li>Type and usage of web site (dynamic, static, Internet store, etc.)</li>
<li>Performance required (response time)</li>
<li>Size of storage</li>
<li>Network speed</li>
</ul></li>
<li>Identify suitable web CMS and web hosting company (unless for the organisation use, taking into various factors, including:
<ul>
<li>Prices</li>
<li>Backup service</li>
<li>Facilities offered (storage, network bandwidth, CPU speed, etc.)</li>
</ul></li>
<li>Prepare purchasing document, in accordance with organisation procurement procedures, and recommendation for supervisor approval</li>
<li>Liaise with hosting service provider to setup DNS reference to the organisation’s new web site and acquire hosting servers logon details to administer the CMS</li>
<li>Download and perform remote installation web CMS on hosting server</li>
<li>Access administrative functions of web CMS to perform following tasks:
<ul>
<li>Upload and install a template for the website</li>
<li>Upload company logo and other media (pictures and video) contents for the home page</li>
<li>Edit the home page with CMS editor</li>
</ul></li>
<li>Test the web site with different web browsers to ensure compatibility</li>
<li>Create login accounts and provide tutorial sessions for web designers to use the CMS editor to create web pages on the web site</li>
</ul>
3. Exhibit professionalism
<ul>
<li>Be familiar with W3C web standards and ensure the CMS and web site are W3C compliant</li>
<li>Always look after the interest of the organisation when dealing with external parties</li>
</ul></td></tr>
</table>

Unit of Competency

Functional Area: Web Support

Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Fully comprehend the requirements of the type of web site the organisation is building and acquire sufficient technical details to subscribe to a web hosting service • Install the CMS on the hosting server and be able to use the CMS editing tools to create the web site’s home page that is compatible with common web browsers • Provide sufficient tutorial and assistance to web page designers that enable them to construct other web pages without any difficulties
Remark	

Unit of Competency

Functional Area: Web Support

Title	Maintain website
Code	107912L3
Range	This unit of competency applies to IT personnel who are responsible to maintain the organisation's website. The website is the window of companies to the Internet world. It represents the organisation. Hence, it is essential to be always in operation and the contents are update without any embarrassing issues, such as customer cannot complete purchasing transaction or students cannot upload (hand in) projects or homework. This UoC concerned with the website maintenance of the content rather than the physical server which the website is hosted on.
Level	3
Credit	3
Competency	Performance Requirements 1. Knowledge for maintaining website: • Possess interpersonal and coordination skills • Possess basic knowledge of principles of website design and maintenance • Possess good knowledge of creating web contents • Possess basic knowledge of operating common web browsers • Possess good knowledge of operating website testing tools • Understand user feedbacks or complaints related to the website • Understand the organisation's website performance requirements • Possess basic knowledge of the organisation document standards and procedures

Unit of Competency

Functional Area: Web Support

Competency	2. Maintain website • Coordinate with various parties in the organisation to implement new features, upload new contents to website • Create various channels to receive information related to the organisation's website, included but not limited to the following: • Visitor feedbacks or user complaints • Results of website testing tools • Monitoring/log statistics • Alerts of website outage • Periodically perform tests including but not limited to the following: • Access to the website is still possible • Web contents are compatible with different browsers and different clients (mobiles and desktops) • No broken links • Software are updated • Access and download speed • Functions/features are operational as expected, such as: checkout, blog, forum, registration, upload, download, etc. • Correct or coordinate with appropriate parties to correct any detected issues and remove redundant contents • Collect visitor traffic statistic for security purpose and/or business use • Pages entered on and exited on • Time spent on the site • Bounce rate • Referring sites • Countries of visitors are from • Use monitoring tools for "Reputation management" of the organisation's name, brands and contents of the website appeared on the Internet, such as Google alert • Apply backup strategies: • Perform scheduled backups • Perform drills for recovery, in the event of website corruption • Document and create reports that comply with the organisation's standards and procedures for assisting website developers and management decision making 3. Exhibit professionalism • Look after the interest and reputation of the organisation • Apply industry best practices and web technologies when maintaining website • Adhere to Intellectual Properties and copyright laws
Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Use different tools to monitor and test organisation's website • Liaise with appropriate parties to correct issues and ensure the website is fully functional, updated and tested with different browsers on different clients • Ensure the website is well backup according to the organisation's planned schedules and can be recovered within the organisation standard
Remark	

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

1. Title	Develop information security standard, policies and guidelines for the organization
2. Code	111164L6
3. Range	This UoC applies to the arrangements and procedures relating to the establishment of information security policies for the organization. This step is to ensure that all staff members have standards to follow and protect the organization from cyber attack, unauthorized access, alteration, unauthorized disclosure, etc.
4. Level	6
5. Credit	6 (for reference only)
6. Competency	Performance Requirements 6.1 Possess the knowledge in the information security area ● Realise the necessity in the establishment of a set of information security policies to be embedded into the organization ● Recognise the changes in cyber technology in the organization’s related industries, and apply the knowledge to analyse future trends and developments in information security threats and measures based on incomplete information collected from different sources ● Understand the compliance requirements and based on that to determine regulatory requirements and obligation under different jurisdictions ● Understand the business requirements of key stakeholders and analyse views collected from different business and operation units accurately to discern their needs in IT control or security 6.2 Develop relevant standard, policies and guidelines ● Establish strategic objectives and compliance position for information security of the organization to provide protection with an outlook of future perspective ● Establish IT control or security (e.g. network) policies with respect to the organizations business strategies and security needs ● Ensure the information security policies and guidelines are established correctly, positioned at the appropriate level, and comprehensive enough for employee to follow 6.3 Develop professional behaviour and attitude

	● Direct communication and training programs on information security measures; ensure all levels of staff are aware of their importance and participate in the protection of information security ● Ensure all information security policies established comply to all existing legal and regulatory requirements as well as social concerns ● Design monitoring measures to ensure compliance with established security policies
7. Assessment Criteria	The integral outcome requirements of this UoC are: ● Formulation of security policies. The policies should be based on critical analysis of a broad range of data and incomplete information with the aim to provide enough protection to organizations' IT systems and meet the regulatory requirements without hampering operational efficiency ● Production of supporting measures on enforcing security policies. Comparison of different types of security measures should be provided to support the design.
8. Remark	

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

1. Title	Review key controls metrics regularly to fulfil the security standard
2. Code	111166L6
3. Range	This UoC involves reviewing key controls metrics to ensure the cybersecurity governance framework stay up to date with current industry practice
4. Level	6
5. Credit	3 (for reference only)
6. Competency	Performance Requirements 6.1 Understand the organisation's security standard, the best practices and industry standards of information security ● understand the security standard ● identify benchmark for assessing the key controls metrics ● be aware of the right cybersecurity practice and industry standards for the organisation 6.2 Review key controls metrics to maintain security standards ● review key control metrics against industry benchmarks ● criticise and identify deficiency of current key controls metrics ● suggest changes to key controls metrics or adaptation of industry best practice to ensure security standards are withheld. ● ensure that the review is done at least periodically and also on need basis 6.3 Exhibit professionalism ● comply with the organisation'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 UoC are the abilities to： ● review key controls metrics against industry benchmarks and criticise or identify deficiency of current key controls metrics ● make suggestions to ensure the key controls metrics could withhold security standards and stay updated with industry development.
8. Remark	

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

1. Title	Design the evaluation criteria security test plans
2. Code	111168L6
3. Range	Design evaluation criteria for security test plans that are tailor to an organization’s needs and risks in relation to industry standards
4. Level	6
5. Credit	3 (for reference only)
6. Competency	Performance Requirements 6.1 Understand the organization’s cyber security standards and practices ● Be able to associate the organization’s business operations and its cyber security standards and practices 6.2 Understand the organization’s cyber security requirements and the likelihood of attack for different vulnerabilities of the organization’s industry ● Be able to ■ identify the important areas for protection ■ identify different kinds of vulnerabilities ■ assess the likelihood of different types and forms of cyberattack 6.3 Set up a benchmark for acceptable cybersecurity level ● Be able to ■ rank the importance of different vulnerabilities and preventative measures in associate to the organization’s IT systems ■ understand associated industry standards 6.4 Set up the evaluation criteria to assess security test plans ● Be able to evaluate and benchmark different preventative measures against industry standards by accounting for the importance of different vulnerabilities in relation to the organization
7. Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to： ● identify the needs and risk of an organization under cyberattacks ● identify the industry standards for the associated vulnerabilities and preventative measures ● establish the set of evaluation criteria, which if satisfied, could greatly minimise the cybersecurity risk of the enterprise
8. Remark	

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

1. Title	Conduct investigation of Information Security Incidents
2. Code	111169L5
3. Range	This UoC involves Investigating information security issues for the organisation, collecting evidences and documenting the activities conducted
4. Level	5
5. Credit	3 (for reference only)
6. Competency	Performance Requirements 6.1 Understand forensics concepts and investigation techniques for the IT systems involved ● Be able to: ■ Evaluate different issues in IT security in order to develop the framework of investigation plan ■ Evaluate different investigation approaches in order to develop the procedures in conducting an investigation of security cases ■ Demonstrate professional knowledge in the various techniques in evidence gathering ■ Understand the functions and operations of the systems involved in the incident 6.2 Investigate security case in a professional manner ● Be able to: ■ 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 ■ Develop investigation plan that define the procedures and techniques used in information collection and documentation of forensic activities ■ Examine the collected data and recognize essential elements of possible forensic activities
7. 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
8. Remark	

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

1. Title	Develop procedures to implement incident response plan
2. Code	111170L5
3. Range	This UoC involves designing the process to implement the incident response plan while minimising the impact on the organisation's operation
4. Level	5
5. Credit	3 (for reference only)
6. Competency	Performance Requirements 6.1 Understand incident response plans ● Understand the processes and operations of the incident response unit ● Aware of the potential scale of incidents and personnel that could potentially be involved ● Understand the tasks that are needed to carry out to have the plan implemented ● Understand the organisation's cyber security policies and assets/infrastructures that could be involved (e.g. Internet of Things, Cloud storage, networks etc.…) 6.2 Develop procedures and guidelines to implement incident response plan ● Determine the responsibility of all associated personnel ● Determine the scale of the tasks that needed to carry out ● Decide the order of the tasks needed to carry out to minimise any interruption to the organisation's operation ● Communicate with relevant departments to understand their needs such that the execution could be planned accordingly to minimise the impact on the organisation's operation ● Ensure that tools and equipment needed for the implementation are all identified and have a plan to make them available for the tasks ● If downtime of essential services are unavoidable, potential backup services should be considered 6.3 Exhibit professionalism ● Comply with the organisation's guidelines and procedures as well as any (local and international) laws and regulatory requirements, if applicable

7. Assessment Criteria	The integrated requirements of this UoC is the ability to design the procedure to implement incident response plan such that impact on the organisation’s operation could be minimised
8. Remark	

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

1. Title	Develop procedures to maintain and comply with the information security standard and policies of the organization
2. Code	111171L5
3. Range	Develop information security practices and procedures for using information systems to comply with the organisation's information security policies
4. Level	5
5. Credit	3 (for reference only)
6. Competency	Performance Requirements 6.1 Understand the organisation's information security policies and operation ● Be able to ■ understand the organisation's information security policies ■ understand the needs and usage of the organisation's information system 6.2 Develop relevant practices, procedures and guidelines to support the policies ● Be able to work with relevant departments to develop detailed practices, procedures and guidelines that support the organisation's information security policies 6.3 Ensure the practices, procedures and guidelines are properly approved ● Be able to explain the practices, procedures and guidelines to user management and get their approval
7. Assessment Criteria	The integrated requirements of this UoC is the ability to develop the practices, procedures and guidelines that comply with the information security standards and policies.
8. Remark	

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

1. Title	Evaluate the results of application security assessment for improvement recommendation
2. Code	111173L5
3. Range	Evaluate the results of application security assessment and propose possible directions for security improvement.
4. Level	5
5. Credit	3 (for reference only)
6. Competency	Performance Requirements 6.1 Knowledge of the requirements of application security assessment ● understand the basic principles, methodologies and tools in the application security assessment process (e.g. RASP, MAST) ● appreciate the objectives of the security assessment ● understand the requirements and goals of the security assessment of the organization 6.2 Evaluate the results of application security assessment ● any security weaknesses and vulnerabilities in source code ● any security weaknesses in architecture, design, open source and third-party components ● consolidate the impacts from possible application security risks in qualitative and quantitative terms ● properly document the evaluation results 6.3 Propose possible directions for improvement ● develop a structured plan to coordinate security improvements in according to the organization's guidelines and requirements ● propose best practices for security assessment ● develp training programmes for internal staff to upgrade their competency
7. Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to： ● critically evaluate the results of application security assessment ● propose possible directions for security improvement in according to the organization's guidelines and requirements
8. Remark	

Specification of Competency Standards for the Information & Communications Technology Industry

Unit of Competency

1. Title	Evaluate the potential security threats to the organisation
2. Code	111174L5
3. Range	This UoC involves evaluating threats that could severely impact an organisation's business processes.
4. Level	5
5. Credit	6 (for reference only)
6. Competency	Performance Requirements 6.1 Understand information resources of an organisation ● understand how information resources of an organisation are handled and can be used to support its normal business processes (including its employees, business assets, business operations and business functions) ● understand the process of how information is acquired and stored within the organisation ● articulate the critical information resources for an organisation's business operation ● explain why certain information resources in an organisation are critical to its business processes 6.2 Determine potential risk factors related to information resources ● identify and analyse risks (such as threats, vulnerabilities and exposures associated with confidentiality, integrity and availability of information resources) that are related to the information resources, information systems and information acquisition process of an organisation, which may have adverse effects on its business processes 6.3 Apply quantitative and qualitative methods to determine sensitivity and criticality of information resources and systems, and the impact of potential adverse events 6.4 Evaluate the potential security threats to the organisation in a professional manner ● apply risk identification and analysis methods to identify physical and logical threats that could severely impact an organisation's employees, business assets, operations and business functions ● evaluate the potential impacts that may arise from those identified threats ● comply with the organisation's policies and guidelines as well as any (local and international) laws and regulatory requirements, if applicable

7. Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to： ● identify threats that could severely impact the organisation ● evaluate the potential impacts that may arise from those identified risks in accordance with the organisation’s policies and guidelines, as well as any (local and international) laws and regulatory requirements, if applicable
8. Remark	

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

1. Title	Perform network security assessment for the organization
2. Code	111176L5
3. Range	Conduct network security assessment by abiding to the organization’s security policy and assessing whether it could protect the organization’s interest.
4. Level	5
5. Credit	6 (for reference only)
6. Competency	Performance Requirements 6.1 Possess the knowledge in the subject area ● Understand the organisation's security policy ● Understand the organisation's business needs ● Be familiar with network infrastructure and all the services that it supports ● Possess extensive knowledge in security principles, implementation of controls and best practices ● Possess extensive knowledge of various security risks, such as possible methods of attacks on signalling layer, database of subscribers, network elements, gateways, frauds, service interruptions, etc. ● Knowledgeable in network security standards and benchmarks ● Knowledgeable with network access requirements of products and services 6.2 Assess network security risks and appropriateness ● Be able to: ■ Work with appropriate departments to determine network access requirements for internal and external users or products and services ■ Assess whether personnel have the appropriate access right ■ Assess whether the network setting could fully impose the organisation's cyber security policy ■ Assess whether the network security is sufficient in minimising risks and protect the core operations and interest of the organisation ■ Document the assessment for record ■ Inform the associate personnel of the result for further processing 6.3 Exhibit professionalism ● Always look after the interest of the organisation as well as customers.

	● Always respect the privacy of the employee when conducting the network security assessment ● Follow the policy and guidelines of the network security assessment
7. Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to： ● conduct the network security assessment abiding to the policy and guidelines ● assess the network security on whether it could protect the interest of the organisation ● document the assessment and inform associate personnel for follow up
8. Remark	

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

1. Title	Prepare and deliver information system security audit report
2. Code	111177L5
3. Range	Report findings after information system security audit work to management via full documentation and management summary in an industry standard format. Make suggestions when necessary to enhance the information system security
4. Level	5
5. Credit	6 (for reference only)
6. Competency	Performance Requirements 6.1 Understand the information system audit work performed with its findings and conclusions ● Be able to identify the key issues in information system security audit work performed that complies with information security policy and standards ● Understand the needs and the considerations involved for the different activities conducted through the information system security audit exercise 6.2 Prepare an information system security audit report ● Be able to provide a report that ■ states the scope, objectives, nature and period of coverage, timing and extent of the audit work performed ■ states the findings, conclusions and recommendations and any reservations, qualifications or limitations ■ When possible, benchmark the findings with industry standards ■ supports the reported results with sufficient and appropriate audit evidence 6.3 Deliver the information system security audit report ● Be able to issue and distribute the report according to the terms of the audit charter 6.4 Provide the information system security audit report identifying major security exceptions and ensure appropriate management follow up actions taken ● Be able to ■ report and alert management if the organisation’s baseline information security governance has been breached ■ ensure appropriate follow up actions has been taken

	■ suggest improvement in future information system security audit work
7. Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to： ● prepare and deliver the information system security audit report in compliance with information security governance and up-to-date industry standards. ● make suggestions on changes to the system to address the issues and to further enhance the information system security
8. Remark	

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

1. Title	Prepare documentation to report the security testing and findings
2. Code	111178L5
3. Range	Follow procedures for documenting for security testing and findings and identify potential follow up actions
4. Level	5
5. Credit	3 (for reference only)
6. Competency	Performance Requirements 6.1 Understand the basis of documenting an event as a basis for subsequent action ● Be able to ■ determine the scope for documentation ■ understand the procedures to document a security test and findings 6.2 Preparing the documentation to report a test or finding ● Be able to ■ ensure that all associated information and results are included ■ state the findings and results and their potential implications ■ identify any potential follow up actions ■ identify the person-in-charge to coordinate all documentation ■ follow organization’s standard procedure and templates in preparing the documentation
7. Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to： ● document the testing and findings in a standard manner ● ensure potential implications are highlighted for possible follow-up actions
8. Remark	

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

1. Title	Propose appropriate countermeasures to prevent security attacks
2. Code	111179L5
3. Range	Ensure that internal and external information technology resources are secured by complying with the organization’s cyber security policy and protect the organization’s interests
4. Level	5
5. Credit	3 (for reference only)
6. Competency	Performance Requirements 6.1 Understand the needs for internal and external resources for information security ● Be able to identify and recognise the internal and external resources that could be compromised and posed as a risk to the organizations interests. 6.2 Identify the strengths and weaknesses of the internal and external resources for cyber security ● Be able to analyse and evaluate the characteristics, nature, limitations, strengths and weaknesses of the internal and external resources ● Be aware and up to date with new security attack methods and new cybersecurity technologies 6.3 Designing and proposing appropriate countermeasures to enhance cyber security ● Address the weaknesses and deficiencies of the system by designing appropriate countermeasures to protect the resources ● Propose update on the systems against new threats and enhance cyber security effectiveness with new technologies
7. Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to： ● identify and optimise both internal and external resources and their weaknesses ● stay up-to-date with new threads and new cybersecurity technologies ● propose new countermeasures by adopting new technologies and techniques to enhance and enforce the cybersecurity
8. Remark	

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

1. Title	Review the possible causes of the threats for remedial actions recommendation
2. Code	111180L5
3. Range	Propose remedial actions that address the possible causes of the threats and minimise interruptions to the organisation’s normal business operations
4. Level	5
5. Credit	6 (for reference only)
6. Competency	Performance Requirements 6.1 Understand the system’s operation, the reporting/recommendation procedures and the organisation’s structure 6.2 Understand the possible causes of the threads ● Be able to ■ judge the validity of the proposed possible causes ■ understand the potential implications of the possible causes ■ evaluate the seriousness of potential causes 6.3 Know the information security emergency management practices (See Remark) ● Be able to understand remedial actions that include processes to organise, train and equip the teams and brief any associated personnel involved in the threats 6.4 Design and propose remedial actions ● Be able to ■ design and propose remedial actions that minimise interruptions of the normal business operations of the organisation ■ design and propose remedial actions that eliminate the possible causes of the threats ■ design and propose remedial actions that include processes to organise, train and equip the teams and any associated personnel involved in the threats to avoid similar causes in the future ■ identify potential equipment or information system infrastructure needed that could minimise the occurrence of similar future cases 6.5 Develop remedial actions in a professional way ● Be able to ensure that the proposed remedial actions comply with

	the organisation’s policies and guidelines as well as any (local and international) laws and regulatory requirements, if applicable
7. Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to： ● design and propose remedial actions that minimise interruptions of the normal business operations of the organisation; ● design and propose remedial actions that eliminate the possible causes of the threats; and ● ensure that the proposed remedial actions comply with the organisation’s policies and guidelines as well as any applicable local and international laws and regulatory requirements.
8. Remark	Examples of information security management practices are production of change control activities and development of computer emergency response team.

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

1. Title	Appraise Open-source intelligence (OSINT) methodology in the security process
2. Code	111181L5
3. Range	Assess the sutiability, advantages and disadvantages of OSINT methodology in the application of the security process of an organization
4. Level	5
5. Credit	3 (for reference only)
6. Competency	Performance Requirements 6.1 Understand the application of OSINT methodology in the security process ● Understand what OSINT methodology is ● Recognise the needs of OSINT in the security process ● Understand the advantages of OSINT methodology in the security process ● Be aware of the industry standards in the related field ● Know of alternative methods in the security process ● Aware of the tools and techniques in applying OSINT methodology in the security process 6.2 Determine the suitability of OSINT methodology in the security process of an organization ● Understand how OSINT could change the organization’s security process ● Determine the needs and requirements of the organization’s security process ● Assess the advantages and disadvantages of OSINT methodology in relation to the organization’s operation 6.3 Set up benchmark and evaluation criteria to assess the OSINT methodology ● Be able to ■ rank the different OSINT sources in relation to the organization’s business setting and standards ■ evaluate and benchmark the OSINT methodology in security processes in relation to other alternatives
7. Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to： ● determine the impact of the application of OSINT methodology on the organization’s security process ● evaluate and benchmark the OSINT methodology in security processes

8. Remark	

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

1. Title	Appraise the security threats in emerging technologies
2. Code	111182L5
3. Range	This UoC involves appraising the potential security threats associated with a range of emerging technologies
4. Level	5
5. Credit	3 (for reference only)
6. Competency	Performance Requirements 6.1 Understand the security threats associated with emerging technologies ● Be able to differentiate the threats associated with emerging technologies with traditional threats ● Be able to scope out various potential security threats by a range of emerging technologies, including but not limited to: ■ Data Breaches ■ Insider Threats ■ Insure Interfaces ■ Hijacking of Accounts ■ Misconfiguration and inadequate change control ■ Security Architecture and strategy ■ Access and Key Management ■ Fake Base Stations ■ IoT Device Hijacking 6.2 Appraise the security threats of the execution of emerging technologies ● Be able to appraise the security threats of the execution or emerging technologies in compliance with industry best practices and standard, including but not limited to: ■ Shared Responsibility Model ■ Data Governance Framework ■ Sensitive Data Protection ■ Audits and Penetration Testing
7. Assessment Criteria	The integrated outcome requirement of this UoC is the ability to appraise the security threats in the execution of emerging technologies in compliance with industry best practices and standards.
8. Remark	

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

1. Title	Compare the strengths and weaknesses of different cryptographic algorithms and determine the suitable algorithm for the organization operation
2. Code	111183L5
3. Range	Identify the cryptographic algorithms that best suit the needs of the organization's operation
4. Level	5
5. Credit	6 (for reference only)
6. Competency	Performance Requirements 6.1 Understand the needs and operation of the organization ● Identify the needs and use cases of cryptographic algorithm within the organization's structure ● Identify the types, sizes and amount of information that need to be encrypted ● Identify the level of security needed for the organization's use case 6.2 Aware of the different cryptographic algorithms and their strength and weakness ● Understand the different cryptographic algorithms available ● Aware of the potential cost of adopting a particular algorithm (such as capital cost, training cost, staff training cost, etc…) ● Understand the industry standards in cryptographic algorithms and how each of the cryptographic algorithms identified performed under these standards ● Understand the complexity of each cryptographic algorithms under consideration ● Aware of the difficulties that each cryptographic algorithms may inflict on the management and user-friendliness of the information ● Identify the strength and weaknesses of different cryptographic algorithms 6.3 Suitability to the organization ● Assess each cryptographic algorithms in consideration against the requirements/needs of the organization ● Consider the total cost incurred on the organization in the adaptation of an algorithm ● Consider the management of the data, the difficulties and effectiveness of implementing each cryptographic algorithms into the organization's operation systems ● Propose to the organization's management the cryptographic algorithm best suited the needs of the organization's operation

7. Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to： ● summarize the strengths and weaknesses of each cryptographic algorithms under consideration with respect to the organization’s operational needs ● propose the cryptographic algorithm that most suited the operational needs of the organization
8. Remark	

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

1. Title	Apply suitable network development tools in the deployment of secure network system
2. Code	111190L4
3. Range	This UoC involves application of suitable network development tools based on the organisation's requirements and limitations for the deployment of a secure network system
4. Level	4
5. Credit	3 (for reference only)
6. Competency	Performance Requirements 6.1 Possess knowledge in the field ● Know the industry standards on secure network system deployment ● Aware of the different network development tools available ● Know the strengths and weaknesses of different network development tools 6.2 Understand the requirements for deployment of a secure network system ● Understand the organisation's requirements, limitations and constraints on the deployment of a secure network system 6.3 Apply suitable network development tools for secure network system deployment ● Select the network development tools that are most suitable for the organisation based on the strengths and weaknesses of the different tools and the requirements and limitations of the organisation ● Use the selected tools for deploying the secure network system 6.4 Perform the tasks in a professional manner ● Minimise disturbance to the organisation's operation ● Comply with the organisation'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 UoC are the abilities to： ● apply the network development tools that are most suitable for the organisation to deploy a secure network system ● Perform the tasks in a professional manner
8. Remark	

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

1. Title	Perform application security assessment for the organisation
2. Code	111191L4
3. Range	Conduct application security assessment for the organisation and suggest recommendations and follow-up action to enhance application security
4. Level	4
5. Credit	3 (for reference only)
6. Competency	Performance Requirements 6.1 Possess the knowledge in the subject area ● Understand the target of the assessment and the tasks that needed to be performed for the assessment ● Understand the importance of allocating the appropriate level of resources for performing the assessment ● Understand that the assessment should be conducted by qualified personnel with relevant experience and expertise ● Understand the needs of application security assessment ● Be aware of the different available approaches and methodologies to carry out the assessment, with their advantages and shortcomings 6.2 Carry out the application security assessment ● Be able to: ■ Define in advance the scope and coverage of the assessment, and consolidate all details into a testing plan ■ Communicate and inform associated units to notify them of the assessment to minimise potential interruption to the organisation’s operation ■ Fully consider critical factors while preparing and planning for the assessment ■ Carry out the tasks planned for the application security assessment ■ Document results and findings of the assessment ■ Identify recommendations and follow up actions from the assessment result if necessary 6.3 Exhibit professionalism ● Ensure all related staff members contribute their greatest effort and honesty in activities related to the assessment

	● Always strike a balance of interests between customers, employees and the company as a whole ● Minimise disturbance to the organisation’s operation ● Comply with the organisation’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 UoC are the abilities to： ● successfully perform the application security assessment for the organisation ● communicate with associated personnel to minimise disturbance to the organisation’s normal operation ● correctly interpret findings from the assessment and propose appropriate recommendations and follow up actions
8. Remark	

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

1. Title	Carry out the first line of communication for triggering client response and alert internal security teams
2. Code	111192L4
3. Range	Ensure the first line of communication is developed for client response and alert internal security teams in a timely manner
4. Level	4
5. Credit	3 (for reference only)
6. Competency	Performance Requirements 6.1 Understanding of the cybersecurity system of the organisation ● Understand the triggers of the system ● Understand the cybersecurity policy of the organisation ● Understand the needs and functions of client response ● Know the functions and work departments of the internal security teams 6.2 Carry out the first line of communication ● Aware of when the first line of communication needs to be developed ● Ensure that the communications are carried out in a timely manner ● Make sure that all associated personnel are kept informed and stay up to date with the incident ● All communications should be recorded and filed for record 6.3 Exhibit professionalism ● Comply with the organisation’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 UoC are the abilities to： ● Ensure that the communications are carried out in a timely manner and are recorded for future reference ● Make sure that all associated personnel are kept informed and stay up to date with the incident
8. Remark	

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

1. Title	Maintain security files by receiving, processing and filing the system data
2. Code	111193L4
3. Range	Ensure the security files received are processed according to the organisation's standard procedures and filled for future reference.
4. Level	4
5. Credit	3 (for reference only)
6. Competency	Performance Requirements 6.1 Understand the data system ● Know the importance of maintaining the system data ● Aware of the filing structurer 6.2 Maintain security files ● Assign unique file numbers for security files ● Ensure the files can be sorted or find easily by the nature of the case for future references, such as by assigning descriptive tags or searchable keywords to the files ● Ensure the filing of the data are done following the organisation's standard procedure ● Process the file in a timely manner ● Grouping all associated data together or linking them for trackability 6.3 Summarising and follow up on security files ● Provide a periodic summary report (monthly, quarterly or half-yearly, depends on the organisation's needs) to show the number of different cases received to assess cybersecurity system effectiveness and for future performance improvement ● Follow up on missing information/data ● Ensure that associated personnel are informed of any required follow up action or the completion of the filing of a case 6.4 Exhibit professionalism ● Comply with the organisation'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 UoC are the abilities to： ● Ensure the filing of the data are done following the standard procedure and that they can be searched easily ● Follow up on missing information and inform the associated personnel of the status of the filed case or follow-up action

	required. ● Create a summary report for management to show the number of incidence within a period to assess the effectiveness of the cybersecurity system and future improvements.
8. Remark	

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

1. Title	Monitor and perform the system security access checking
2. Code	111194L3
3. Range	Follow the organization's policy to monitor and protect the security elements associated with information of an organization.
4. Level	3
5. Credit	3 (for reference only)
6. Competency	Performance Requirements 6.1 Knowledge for monitoring the system security access ● understand the importance of access security checking to the organization operations and thus, the demand for proper handling ● understand the scope and areas for the access security checking within the organization's overall security infrastructure ● consider the critical factors of the access security control such as password control and related administrative arrangements ● review the available techniques and methodologies for access security checking with their own advantages and shortcomings 6.2 Carry out the system security access check ● apply appropriate tools to carry out the access checking ● closely monitor the effectiveness of the checking process ● follow the organization's guidelines to handle any malfunctions of system security access and report to the organizatino's management 6.3 Exhibit professionalism ● communicate with different stakeholders effectively and skillfully such that they know the organization's policies regarding access security checking ● strike a proper balance of interests between customers and the organization as a whole
7. Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to： ● ensure all access security checking tasks will be executed effectively and correctly ● follow the organization's guidelines to handle any malfunctions of system security access
8. Remark	

Specification of Competency Standards for the Information and Communications Technology Industry

Unit of Competency

1. Title	Manage IT service management strategy
2. Code	111204L6
3. Range	Coordinate the IT service management system documentations and monitor processes to adhere to standard
4. Level	6
5. Credit	3 (for reference only)
6. Competency	Performance Requirements 6.1 Possess knowledge of IT service management ● Understand the operations and processes involved in IT service ● Understand the importance of cybersecurity in IT service ● Understand the various factors, e.g. objectives and goals, success criteria, cost drivers, performance measurements, cybersecurity etc., affecting IT services for an organisation ● Understand the various needs of IT services in an organisation ● Understand IT tools and systems available in managing IT services 6.2 Apply the knowledge of IT service management in an organisation ● Monitor IT service activities involved in IT operations and IT processing ● Maintain documentation of IT services ● Make use of IT tools and systems in the management of IT services 6.3 Enhance the effectiveness and efficiency of IT services in an organisation ● Monitor IT service activities to ensure they are carried out in a timely manner ● Ensure IT services are devlivered securely and up to standards ● Make appropriate changes to the systems or processes to enhance the effectiveness and efficiency of IT service management ● Manage the IT activities involved in the most effective and efficient manner for the organisation ● Demonstrate that the IT services of an organisation is achieving the set objectives and goals
7. Assessment Criteria	The integrated outcome requirements of this UoC is the abilities to demonstrate the IT services are well managed and under control in the organisation in order to meet its business goals and objectives
8. Remark	This UoCs is related to and may overlap with UoCs defined in the Operations & Support functional area.

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

1. Title	Review and comply with organisational policies and procedures, relevant laws and regulatory requirements
2. Code	111205L6
3. Range	This UoC involves reviewing practices to ensure that the service delivered adhere to the organisational policies and procedures, relevant laws and regulatory requirements
4. Level	6
5. Credit	6 (for reference only)
6. Competency	Performance Requirements 6.1 Have knowledge of organisational practices, infrastructures, policies and procedures ● know the operational structure of the organisation ● aware of the different technologies, tools, equipment and online services that are related to the service or tasks delivered ● understand the organisation's policies, procedures and goals ● observe organisational practices and procedures 6.2 Have knowledge of relevant laws and regulatory requirements related to the industry of the organisation ● comprehend the latest regulatory requirements applicable to the organisation, including but not limited to: ■ Intellectual property right protection ■ Personal data (Privacy) ordinance ■ National security law ■ Telecommunications ordinance ● refer to the appropriate experts for guidance where necessary 6.3 Review and comply with organisational policies and procedures, relevant laws and regulatory requirements ● Identify the applicable laws and compliances ● observe and adhere to relevant policies and procedures, laws and regulations in an efficient and effective manner ● take the initiative to improve the organisation's policies and procedures where appropriate ● obtain the endorsement of relevant stakeholders ● obtain prior approvals for system resources and access, such as communication protocols and ports, data storage, online services,

	other system peripherals, computer time as well as data of another person ● review practices, identify and rectify any noncompliance procedures ● make use of tools, infrastructures, equipment and online services available to enhance the service delivered ● make suggestions to enhance existing or purchase of new tools, infrastructures, equipment and online services if it helps to improve on the compliance to related regulations or the effectiveness of the service delivered ● make effective and efficient use of external experts where necessary to meet its business goals and objectives ● report serious misconducts and noncompliance procedures to relevant management and suggest methods to avoid future occurrences (such as provide training programs or workshops to highlight issues to relevant personnel)
7. Assessment Criteria	The integrated requirements of this UoC are the abilities to： ● review of own practices; identify and rectify any noncompliance procedures ● comply to organisational policies and procedures, relevant laws and regulatory requirements ● obtain prior approval for system access and resources according to the aforementioned policies and requirements ● Utilise existing resources and make suggestions on updating or acquiring new resources to enhance the service delivered and adhesion to various related policies and regulations ● Report serious misconducts and noncompliance procedures to relevant management and suggest methods to avoid future occurrences (such as provide training programs or workshops to highlight issues to relevant personnel)
8. Remark	

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

1. Title	Set policy to control data security and privacy
2. Code	111206L6
3. Range	Establish policy to control data security and privacy of an organisation
4. Level	6
5. Credit	6 (for reference only)
6. Competency	Performance Requirements 6.1 Understand legal requirements on data security and privacy ● locate and make reference to sources of legislation applicable to local business entities (Remark) ● seek professional advices on issues relating to security and privacy 6.2 Observe standards, guidelines and procedures published by professional bodies ● comprehend the standards, guidelines and procedures published by professional bodies in the trade and extract the sections relevant to organisational operation as reference 6.3 Set corporate policy to control data security and privacy ● formulate control policies to cover stages from data capture and processing, information flow and distribution, storage and access to retirement ● formulate control policies to ensure that information is relevant, accurate and timely and its management is an integral part of strategic management ● formulate control policies to maintain confidentiality, integrity, and reliability throughout the stages to comply with administrative, audit and legal requirements 6.4 Keep the policy up to date ● perform regular review on the local and international policies to ensure it meets the changing operational environment ● cross check the policy with current best practice as published by professional bodies in the trade to make optimum use of the information resources 6.5 Set policy to control data security and privacy in a professional manner ● establish the required policies in accordance with organisation's guidelines as well as any (local and international) laws and regulatory requirements, if applicable
7.	The integrated outcome requirements of this UoC is the ability to produce a

Assessment Criteria	policy document addressing the control of data security and privacy.
8. Remark	Some reference sources of legislation applicable to business entities are: ● Bilingual Laws Information System http://www.legislation.gov.hk/eng/index.htm ● Personal Data (Privacy) Ordinance http://www.pcpd.org.hk/english/ordinance/ordfull.html ● General Data Protection Regulation (GDPR) https://gdpr.eu/ ● The Personal Information Protection Law of the Mainland https://www.pcpd.org.hk/english/data_privacy_law/mainland_law/mainland_law.html ● The PRC Data Security Law http://www.hk-lawyer.org/content/new-prc-data-security-law-and-its-potential-impact-overseas-data-transfers

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

1. Title	Review the emerging technologies and cross-functional strategies
2. Code	111207L6
3. Range	Review cross-functional strategies to enable an organisation to identify suitable emerging technologies for supporting its business strategies
4. Level	6
5. Credit	3 (for reference only)
6. Competency	Performance Requirements 6.1 Understand issues associated with emerging technologies ● evaluate the values of the emerging technologies with respect to business-technology alignment and enablement of the organization ● understand the deployment procedures of the emerging technologies ● keep updated of the application development areas of various emerging technologies, including but not limited to: ■ Artificial intelligence and machine learning ■ Cloud computing ■ Internet of things ■ Security and automation ■ Streaming technologies ● aware of the data security and privacy concerns in the domains of various emerging technologies 6.2 Review cross-functional strategies for deploying and managing the emerging technologies ● review the organization business strategies, and conduct a mapping between the possible application areas of emerging technologies with the business strategies ● setup a clear digital strategy, if necessary, to ■ identify the appropriate technology applications for different operations of the organization ■ prioritize projects that require cross-functional collaboration ■ setup the project management team for cross-functional projects
7. Assessment Criteria	The integrated outcome requirements of this UoCs are the abilities to ● conduct a mapping between the possible application areas of emerging technologies with the business strategies ● setup digital strategy to support the deployment and management

	of cross-functional projects
8. Remark	

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

1. Title	Implementing monitoring equipment to monitor infrastructure failure and security breaches
2. Code	111429L4
3. Range	For a network to operate reliably and efficiently, continuous monitoring is required to detect faults and security breaches so that appropriate actions can be taken. This UoC describes the competencies for implementing monitoring equipment to monitor infrastructure failure and security breaches.
4. Level	4
5. Credit	6 (for reference only)
6. Competency	Performance Requirements 6.1 Possess the knowledge in the subject area ● Expert in implementing various types of network monitoring management tools, Internet of things (IoT) device management software, alarm management tools, log management, system messages, software systems ● Knowledgeable of the operational requirements, duties, functions, and procedures of network related systems of the organisation ● Extensively experienced with network monitoring and implementation of monitoring equipment ● Possess in depth knowledge of network infrastructure, diagrams, maps and access network plans ● Possess extensive knowledge of the operating characteristics of the network components ● Understand the organisation's security policy 6.2 Implementing monitoring equipment to monitor infrastructure failure and security breaches ● Be able to: ■ Determine from work orders or supervisors the type of monitoring and objective of performing monitoring thresholds e.g. to meet SLA commitment to customers, to collect statistic for capacity planning, for support purpose, etc ■ Identify the appropriate monitoring equipment to use and consider alternatives ■ Determine and define operating baselines for the network infrastructure or components ■ Acquire trigger criteria from appropriate parities (product owners, network engineers, customers) and configure

	triggering network equipment with the required trigger settings. ■ Ensure that triggers record are documented and alerted the associated personnel ■ Set monitoring equipment to monitor the threshold points. The monitoring equipment should produce the required statistics and report for analysis and, if necessary, trigger alarms ■ Perform simulated tests of the monitoring equipment to verify the setting is correct ■ Fully document the implementation steps with network diagrams showing where triggers start, end, monitoring threshold, etc. Extra user procedures will be required for any internally developed monitoring equipment/software ■ Distribute copies of the document to appropriate parties (supervisor, network engineers, etc.) for vetting and filing in accordance with the organisation standards and procedures ■ Demonstrate the completion of the implementation with test results and acquire stakeholders or supervisor signoff ■ Ensure that all tools implemented are secured and complied with the organisation's cybersecurity policy 6.3 Exhibit professionalism ● Follow safety procedures while configuring and implementing network monitoring equipment ● Ensure documents conform to the organisation's standards and policies ● Always take into consideration and strike a proper balance among all related technological, environmental and legal factors
7. Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to： ● identify and fully understand the monitoring requirements from work orders and/or supervisors ● identify the monitoring factors such as trigger points, threshold, and output requirements (logs, alerts, alarms, etc.) ● correctly select the appropriate monitoring equipment to monitor the network functions and/or security of the network infrastructure ● Ensure all tools implemented are secured and complied with the organisation's cybersecurity policy ● successfully implement the monitoring by setting/adjusting/configuring monitoring devices to record statistics, trigger alarm/alert or send messages ● successfully demonstrate the completion of the implementation of the monitoring equipment with test results and documentation

8. Remark	

Appendix D.4 UoCs in Information Security

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

1. Title	Ensure information security procedures and guidelines support information security policies	
2. Code	ITSWIS402A	
3. Range	Ensure the development of procedures and guidelines support the defined information security policies of an organisation as per ITSWIS601A [Information Security － Information Security Governance]	
4. Level	4	
5. Credit	2	
6. Competency		Performance Requirement
	6.1 Understand information security policies	Be able to ▪ identify the required levels of protection for information resources ▪ identify the responsibilities of relevant persons in protecting the information resources based on the organisation's information security policies
	6.2 Identify the responsibilities of protecting the information resources among all members of the organisation	Be able to share the responsibilities among all members of the organisation in protecting and preserving the information resources and complying with applicable policies and laws through the awareness of the growing importance of securing electronic resources
	6.3 Monitor the development of the procedures and guidelines that support information security policies	Be able to ensure the development of procedures and guidelines to support the information security policies
	6.4 Review and revise procedures and guidelines	Be able to ▪ review the suitability of the procedures and guidelines that support information security policies ▪ revise the procedures and guidelines that support information security for further improvement within a revisable timeframe
	6.5 Ensure the development of procedures and guidelines in a professional manner	Be able to make sure that the development of procedures and guidelines that support information security policies are in accordance with organisation's policies and 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 ensure the developed procedures and guidelines can support information security policies in accordance with the organisation's information security strategy.	
Remark		

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

1. Title	Support and implement information security practices and procedures
2. Code	ITSWIS404A
3. Range	Support and implement the information security practices and procedures for using information systems to comply with the organisation's information security policies [Information Security – Information Security Management]
4. Level	4
5. Credit	2
6. Competency	Performance Requirement 6.1 Understand the organisation's information security policies — Be able to understand the organisation's information security policies 6.2 Implement the practices, procedures and guidelines — Be able to ▪ publish and communicate the practices, procedures and guidelines to the staff responsible ▪ assist user department to resolve issues ▪ report to senior management the implementation status of their approved policies ▪ set up a framework to review the implementation of these policies in accordance with the organisation's policies and procedures as well as any local and international laws and standards
7. Assessment Criteria	The integrated requirements of this UoCs are the abilities to: (i) implement the practices, procedures and guidelines to support the information security policies; and (ii) assist user departments to implement the information security policies.
Remark	

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

1. Title	Conduct drills according to response and recovery plans
2. Code	ITSWIS406A
3. Range	Conduct periodic testings of the response and recovery plans, where appropriate, so as to minimize the impacts of any real security incidents on the organisation [Information Security – Response Management]
4. Level	4
5. Credit	2
6. Competency	Performance Requirement 6.1 Understand disaster recovery testing for infrastructure and critical business applications — Be able to explain the importance of performing regular testings of the response and recovery plans 6.2 Conduct periodic testing of the response and recovery plans — Be able to conduct periodic testings of the response and recovery plans, where appropriate, so as to minimize the impacts on the organisation when real security incidents occur 6.3 Conduct periodic testing of the response and recovery plans in a professional manner — Be able to conduct periodic testings of the response and recovery plans in accordance with the organisation’s policies and procedures, as well as any (local and international) laws and regulatory requirements, where applicable
7. Assessment Criteria	The integrated outcome requirements of this UoCs are the abilities to: (i) conduct periodic testings of the response and recovery plans, where appropriate, so as to minimize the impacts of any real security incidents should they occur in the organisation; and (ii) conduct regular testings of the response and recovery plans according to the organisation’s policies, laws and regulatory requirements, where applicable.
Remark	

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

<table>
<tr><td>1. Title</td><td colspan="2">Evaluate and assess effectiveness of corporate information security practices</td></tr>
<tr><td>2. Code</td><td colspan="2">ITSWIS507A</td></tr>
<tr><td>3. Range</td><td colspan="2">Establish appropriate techniques to measure, monitor and report on the effectiveness of information security practices implemented in information protection, application systems and telecommunications networks
[Information Security – Information Security Management]</td></tr>
<tr><td>4. Level</td><td colspan="2">5</td></tr>
<tr><td>5. Credit</td><td colspan="2">3</td></tr>
<tr><td>6. Competency</td><td></td><td><u>Performance Requirement</u></td></tr>
<tr><td></td><td>6.1 Understand different techniques to monitor and measure the effectiveness of information security practices</td><td>Be able to understand different techniques for monitoring and measuring information security practices</td></tr>
<tr><td></td><td>6.2 Understand different technique for vulnerability assessment</td><td>Be able to
▪ understand the vulnerabilities in non-compliance with information security practices
▪ identify techniques for detecting vulnerabilities
▪ set procedures and guidelines in handling vulnerabilities in non-compliance issues</td></tr>
<tr><td></td><td>6.3 Monitor and measure report on the effectiveness of information security controls</td><td>Be able to
▪ define the monitoring process to perform regular and/or event-driven monitoring process
▪ define the techniques to measure the effectiveness of the information security practices
▪ define the reporting mechanisms on the effectiveness of the information security controls
▪ identify the responsible personnel in the monitor, measure and report processes</td></tr>
<tr><td></td><td>6.4 Ensure the non-compliance issue and other variance are resolved in a timely manner</td><td>Be able to
▪ define the procedures for handling non-compliance issue
▪ define the time frame in handling non-compliance issue
▪ identify the responsible personnel who can ensure the non-compliance issues are resolved</td></tr>
<tr><td>7. Assessment Criteria</td><td colspan="2">The integrated outcome requirements of this UoCs are the abilities to:
(i) establish processes to monitor, measure and report on the effectiveness of information security controls; and
(ii) establish processes to assess the vulnerability in non-compliance with information security policies.</td></tr>
<tr><td>Remark</td><td colspan="2"></td></tr>
</table>

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

1. Title	Ensure availability, integrity and confidentiality of information systems	
2. Code	ITSWIS508A	
3. Range	Implement information security measures for protecting the availability, integrity and confidentiality of information systems/data in the change management process [Information Security – Information Security Management]	
4. Level	5	
5. Credit	2	
6. Competency		Performance Requirement
	6.1 Know how to protect the integrity and confidentiality of information systems/data in the organization	Be able to understand how to keeping information accurate and from being disclosed to unauthorized parties
	6.2 Understand the process of change management	Be able to ensure the proposed changes are merited and will not adversely affect other elements of the organization’s planning
	6.3 Implement security measures for protecting the integrity and confidentiality of information systems/data in the change management process	Be able to organise processes, install software, and set up hardware to ensure the confidentiality and integrity of data, availability of information technology resources owned by the organization and its authorized users. Security measures may include reviewing files for potential or actual policy violations and investigating security-related issues
	6.4 Ensure the organization’s information security is not compromised throughout the change management process	Be able to assure an organization’s information security infrastructure, systems and data are not compromised throughout the change management process in the implementation of security measures
7. Assessment Criteria	The integrated outcome requirements of this UoCs are the abilities to: (i) ensure the integrity and confidentiality of data together with availability of information systems are not compromised throughout the change management process; and (ii) ascertain an organization’s security policies are being complied with.	
Remark		

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

1. Title	Enact information system security audit plan	
2. Code	ITSWIS513A	
3. Range	Execute the information system security audit plan with due care on audit evidence for the organization [Information Security – Information System Audit]	
4. Level	5	
5. Credit	3	
6. Competency		Performance Requirement
	6.1 Conduct the audit assignments according to the information system audit plan	Be able to carry out the information system audit plan
	6.2 Gather sufficient, reliable and relevant evidence to achieve the audit objectives	Be able to gather appropriate audit evidence
	6.3 Interpret and analyse the collected evidence to conclude the audit findings	Be able to analyse audit evidence and draw findings and conclusions
	6.4 Record the process, the evidence, the findings and conclusions of the audit	Be able to maintain proper records of the audit
	6.5 Exercise the audit following appropriate professional standards and ethics	Be able to ensure the information systems audit effectively achieves the audit objectives
7. Assessment Criteria	The integrated outcome UoCs requirements of this UoCs are the ability to conduct information system security audit effectively and professionally.	
Remark		

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

1. Title	Establish corporate information security standards	
2. Code	ITSWIS612A	
3. Range	Promulgate and co-ordinate with services providers or external parties to establish information security practices and ensure their compliance with the enterprise's information security policies [Information Security – Information Security Management]	
4. Level	6	
5. Credit	2	
6. Competency		Performance Requirement
	6.1 Understand the enterprise's information security policies	Be able to understand the enterprise's information security policies
	6.2 Understand the information security requirements for services provided by external parties	Be able to • identify the service providers and external parties and understand their services • assess the information security requirements for their services
	6.3 Advocate and explain the enterprise information security policies	Be able to ▪ explain the enterprise information security policies to external parties ▪ define the IS requirements to external parties ▪ explain the relevant information security policies and practices
	6.4 Establish the information security practices with external parties	Be able to establish the information security practices, procedures and guidelines that support the enterprise's information security policies
	6.5 Set up processes to monitor the compliance with information security policies for the services provided by external parties	Be able to define the monitoring and reporting processes for non-compliance with the established information security practices, procedures and guidelines
7. Assessment Criteria	The integrated outcome requirements of this UoCs are the abilities to: (i) explain the enterprise information security policies to services provider or external parties; (ii) establish the information security practices, procedures and guidelines that support the enterprise's information security policies; and (iii) establish the monitoring and reporting processes for non-compliance with the enterprise's information security policies.	
Remark		

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

<table>
<tr><td>1. Title</td><td colspan="2">Devise processes for detecting, identifying and analysing security incident</td></tr>
<tr><td>2. Code</td><td colspan="2">ITSWIS613A</td></tr>
<tr><td>3. Range</td><td colspan="2">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]</td></tr>
<tr><td>4. Level</td><td colspan="2">6</td></tr>
<tr><td>5. Credit</td><td colspan="2">2</td></tr>
<tr><td>6. Competency</td><td></td><td>Performance Requirement</td></tr>
<tr><td></td><td>6.1 Understand help desk processes</td><td>Be able to
▪ 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</td></tr>
<tr><td></td><td>6.2 Know information security incident detection and reporting policies and processes</td><td>Be able to develop processes for detecting and identifying information security incidents</td></tr>
<tr><td></td><td>6.3 Develop processes to deal with security incidents</td><td>Be able to develop and implement processes for detecting, identifying and analysing security related events of an organization</td></tr>
<tr><td></td><td>6.4 Develop processes to deal with security incidents professionally</td><td>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</td></tr>
<tr><td>7. Assessment Criteria</td><td colspan="2">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.</td></tr>
<tr><td>Remark</td><td colspan="2"></td></tr>
</table>

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

1. Title	Develop an information system security audit plan
2. Code	ITSWIS618A
3. Range	Develop an information system security audit (ISA) plan to aid corporate governance in particular on the use of information systems and data in an organization [Information Security – Information System Audit]
4. Level	6
5. Credit	4
6. Competency	<u>Performance Requirement</u>
	6.1 Understand the functions of ISA and the format of an ISA plan — Be able to plan an ISA exercise
	6.2 Understand applicable laws — Be able to list all applicable legal requirements related to an ISA exercise
	6.3 Understand and evaluate various professional auditing standards — Be able to formulate best practices for an ISA exercise
	6.4 Define the purpose, responsibility, authority, and accountability of the ISA function in Audit Charter — Be able to establish policy for guiding the development and execution of ISA plan
	6.5 Develop an ISA plan that matches the needs of the organization and the characteristics of the information system — Be able to develop an information systems audit plan that ▪ addresses the audit objectives as defined by the stakeholders ▪ describes the audit detailing the nature and objectives, timing and extent, objectives and resources required
	6.6 Develop ISA plan in compliance with applicable laws and professional auditing standards — Be able to ensure the information systems audit plan is effective and in compliance with applicable laws and professional auditing standards
7. Assessment Criteria	The integrated outcome requirements of this UoCs is to develop an information system audit plan based on appropriate adoption of professional standards in order to effectively fulfil the audit objectives as defined by the organization and in compliance with applicable laws.
Remark	Able to document the information system security audit plan is assumed to be a common generic skill.

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

1. Title	Maintain the security control documents	
2. Code	ITSWOS418A	
3. Range	Prepare and maintain the security control documents in the context of providing security management services for the IT operations of an organization (See Remark 1 for the content of security control documents) [Operations and Support – Security Management Services]	
4. Level	4	
5. Credit	2	
6. Competency		<u>Performance Requirement</u>
	6.1 Locate security information sources	Be able to identify and locate security information sources such as: ▪ managerial security policy and guidelines ▪ authorised security control plan ▪ industry best practices from professional bodies of local and international standards
	6.2 Prepare and maintain the security control documents	Be able to ▪ prepare and maintain security control documents which covers security roles and responsibilities, processes, parameter settings / configuration, security reporting, and ongoing support on the operating environment ▪ act as central hub of current security documents of the corporation ▪ keep records of changes, amendments and distribution for audit trail
	6.3 Prepare and maintain the security control documents professionally	Be able to ▪ 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 prepare and maintain the security control documents.	
Remark	1. The security control documents should, at least, cover security roles and responsibilities, processes, parameter settings/configuration, security reporting and ongoing support on the operation environment. 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®.	

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

1. Title	Deliver the security services for operations	
2. Code	ITSWOS521A	
3. Range	Plan, implement, operate and administer the security for infrastructure environment in accordance with the current security policy and guidelines 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	3	
6. Competency		Performance Requirement
	6.1 Have knowledge about operating environment for security management	Be able to ▪ understand the security policy and guidelines from management ▪ recognise the importance of confidentiality, integrity and availability to business in security management processes
	6.2 Understand purposes and practices of the security management process	Be able to ▪ state the primary need is to protect business information against potential risks ▪ adopt the principles of the security management process and its best practices
	6.3 Plan and implement the security for infrastructure environment	Be able to ▪ establish a set of practical and efficient policies and procedures to control and manage the security of the infrastructure environment ▪ define security management processes ▪ draw up a security control plan ▪ seek support from management to implement the security measures ▪ perform the construction of secure infrastructure environment
	6.4 Operate and administer the security for infrastructure environment	Be able to ▪ execute the security management process to protect an infrastructure ▪ monitor and operate the security system that controls infrastructure environment ▪ administer the security system according to established procedures
	6.5 Plan, implement, operate and administer the security for infrastructure professionally	Be able to exercise industry best practices and adhere to both local and international standards
7. Assessment Criteria	The integrated outcome requirements of this UoCs are the abilities to plan, implement, operate and administer the security for infrastructure environment.	
Remark	1. The participant is assumed to have a comprehensive knowledge in IT and its applications. 2. This UoCs comprises both planning and operating the security for infrastructure environment for the security management services of ITIL®.	

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

1. Title	Conduct operation security risk assessment and audit	
2. Code	ITSWOS530A	
3. Range	Perform regular security risk assessment and internal security audit for the operations and implement the recommendations based on result of security risk assessment and audit in the context of providing security management services for the IT operations of an organisation [Operations and Support – Security Management Services]	
4. Level	5	
5. Credit	2	
6. Competency		Performance Requirement
	6.1 Know corporate security requirements and business processes	Be able to ▪ comprehend the given security control plan ▪ demonstrate understanding on user administration and system administration processes
	6.2 Plan for risk assessment and security audit	Be able to ▪ observe schedule requirements on security risk assessment and internal security audit ▪ communicate with target operating units and agree with them on the schedule
	6.3 Perform regular security risk assessment and internal security audit	Be able to ▪ identify and classify the risk affecting the security environment ▪ perform regular security risk assessment ▪ perform regular internal security audit to ensure compliance to established guidelines and procedures ▪ recommend follow up actions to tighten security control
	6.4 Implement the recommendations based on result of security risk assessment and audit	Be able to ▪ assess the cost, benefit and effectiveness of the recommendations ▪ seek endorsement from management on the recommendations ▪ implement the recommendations
	6.5 Perform regular security risk assessment and internal security audit and implement the recommendations based on result of security risk assessment and audit in a professional manner	Be able to ▪ minimize disturbance to target operating units when conducting risk assessment and internal audit ▪ comply with organisation'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) perform regular security risk assessment and internal security audit; and (ii) implement the recommendations based on the results of security risk assessment and audit.	
Remark	1. The participant is assumed to have comprehensive knowledge in IT and its applications. 2. This UoCs comprises both planning and operating the security for infrastructure environment for the security management services of ITIL®.	

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

1. Title	Conduct security investigation	
2. Code	ITSWOS619A	
3. Range	Investigate security incidents to identify any security loopholes / breaches and make recommendations for improvement in the context of providing security management services for the IT operations of an organization [Operations and Support – Security Management Services]	
4. Level	6	
5. Credit	2	
6. Competency		Performance Requirement
	6.1 Familiarise with corporate security issues	Be able to be conversant with corporate security issues such as ▪ security policy and guidelines ▪ security control plan and policy ▪ risk assessment and internal audit processes ▪ routine security check procedures and schedule ▪ distribution of security control documents ▪ procedure to report and contain security threats
	6.2 Investigate security incidents to identify any security loopholes/breaches	Be able to ▪ monitor and control the day-to-day security checking ▪ investigate security incidents to identify any security loopholes/ breaches ▪ make recommendations for improvement
	6.3 Make recommendations for improvement	Be able to ▪ assess the cost, benefit and effectiveness of the recommendations ▪ implement the recommendations
	6.4 Investigate security incidents to identify any security loopholes/breaches and make recommendations for improvement professionally	Be able to ▪ exercise industry best practices and adhere to both 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) investigate security incidents to identify any security loopholes/breaches; and (ii) make recommendations for improvement.	
Remark	1. The participant is assumed to have a comprehensive knowledge in IT and its applications. 2. This UoCs comprises both planning and operating the security for infrastructure environment for the security management services of ITIL®.	