Vocational Qualifications Pathway (VQP) for Cloud Computing

Area Job Level	Cloud Computing
Master Level	*The ICT practitioners at this level are mainly responsible for decision-making processes. They oversee the entire IT operations and strategic development direction in the organizations. The Professionals at this level are required to possess broad corporate perspective, good communication skills and in-depth technology knowledge.*
Relevant Job Titles	Chief Technology Officer
	Director of Cloud Solutions
	General Manager of Cloud Solutions
	Chief Cloud Architect
Specialist Level	*The ICT practitioners at this level are mainly involved in managerial processes. They may work 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 are to manage individual activities and project segments, and to lead the projects towards completion within the assigned budget and stipulated deadline.*
Relevant Job Titles	Cloud Architect
	Cloud Software Engineer
	Cloud Network Engineer
	Cloud Security Engineer
Practitioner Level	*The ICT practitioners at this level manage certain parts of technical processes depending on their subject matter expertise. The professionals at this level may be sub-degree graduates or those who possess certain work experience in the field.*
Relevant Job Titles	Cloud Support Engineer
	Junior Cloud System Analyst
	Junior Cloud Network Engineer
Support Level	*The ICT practitioners at this level provide entry-level technical operation and support functions depending on their subject matter expertise. The practitioners at this level may be S6 graduates with relevant ICT skills and knowledge or those who possess little work experience in the field.*
Relevant Job Titles	Computer Operator
	User Support Staff
	Technical Support Staff (TSS)
	Field Technician
	Help Desk Operator

Proposed Competency Requirements (Cloud Computing - Master Level)

Relevant Job Titles:

- Chief Technology Officer / Director of Cloud Solutions / General Manager of Cloud Solutions / Chief Cloud Architect

Area of Work / Cluster Name	Major Tasks	Competency Requirements	Units of Competency (UoCs) Number	Relevant Qualification for fulfilling Competency Requirements
Cloud Infrastructure Policies and Strategies	1. Lead, define, and design cloud infrastructure strategy and approach while developing and maintaining relationships with key technical client stakeholders	▪ Formulate business strategies and policies	111201L6	Obtain qualification via training programmes (QF Level 6)
		▪ Maintain the portfolio and supply chain management with different stakeholders	111203L6	
		▪ Formulate IT strategies and policies	ITSWSM603A	
		▪ Review the emerging technologies and cross-functional strategy	111207L6	
		▪ Review the ethical and social issues for IT applications	111208L6	
		▪ Conduct solicitation process in project outsourcing	111196L5	
		▪ Conduct source selection and/or contract development	ITSWPM523A	
	2. Define and ensure best practices and compliance to development standards are upheld across teams	▪ Define data governance policies and architecture principles	111123L6	
		▪ Review and comply with organisational policies and procedures, relevant laws and regulatory	111205L6	

Area of Work / Cluster Name	Major Tasks	Competency Requirements	Units of Competency (UoCs) Number	Relevant Qualification for fulfilling Competency Requirements
		requirements ▪ Set policy to control data security and privacy	111206L6	
Planning and Evaluation of requirements for Cloud Infrastructure	3. Advise internal and clients teams on technical challenges and risks, costs and benefits, and alternative solutions	▪ Establish a business case for an IT investment ▪ Prepare a budget based on the IT plan ▪ Conduct solicitation planning ▪ Project the potential costs, benefits and ROI of IT project	ITSWGS617A ITSWSM504A 111197L5 111211L5	(Continued) Obtain qualification via training programmes (QF Level 6)
	4. Develop and map technical requirements for network infrastructure to business goals and needs	▪ Identify and evaluate information technologies that support the objectives of an organisation ▪ Define metrics to ensure that a technology architecture meets the business goals ▪ Formulate IT plan	111202L6 111127L5 111210L5	
Strategic Management	5. Overview and review work of the team (Generic Skills)	▪ Lead and motivate a team ▪ Delegate responsibilities ▪ Manage changes	ITSWGS604A ITSWGS606A ITSWGS613A	

Proposed Competency Requirements (Cloud Computing - Specialist Level)

Relevant Job Titles:

- Cloud Architect / Cloud Software Engineer / Cloud Network Engineer / Cloud Security Engineer

Area of Work / Cluster Name	Major Tasks	Competency Requirements	Units of Competency (UoCs) Number	Relevant Qualification for fulfilling Competency Requirements
Design and administration of Cloud infrastructure	1. Design and administrate the cloud environments	▪ Develop procedures to implement incident response plan ▪ Develop the micro-service architecture ▪ Define the user requirements ▪ Manage organization resources for implementation across multiple processing environment	111170L5 111128L5 111162L4 111163L4	Obtain qualification via training programmes (QF Level 5)
	2. Design, develop, troubleshoot, and debug software programs for enhancements and integration with Cloud solutions	▪ Analyse the performance, latency and accessibility of systems ▪ Ensure operable application integration architecture is in place ▪ Manage application integration architecture life cycle	111130L4 ITSWAR516A ITSWAR517A	
	3. Manage system migration and upgrade to create and deploy new cloud environments	▪ Define a system migration plan ▪ Perform risk assessment on system migration	111155L6 111157L6	

Area of Work / Cluster Name	Major Tasks	Competency Requirements	Units of Competency (UoCs) Number	Relevant Qualification for fulfilling Competency Requirements
Evaluation on Business needs for Cloud infrastructure	4. Perform evaluation, maintenance and installation to ensure the network and infrastructure performance meets business requirements	▪ Establish a business continuity planning strategy ▪ Analyze the available solutions from IT service providers	111209L5 111199L4	Obtain qualification via training programmes (QF Level 5)
Information Security (Cloud)	5. Design security measures that would enhance the security of cloud-based environments	▪ Appraise the security threats in emerging technologies ▪ Formulate data security and consent policy for emerging technologies ▪ Ensure availability, integrity and confidentiality of information systems	111182L5 111186L5 ITSWIS508A	

Proposed Competency Requirements (Cloud Computing - Practitioner Level)

Relevant Job Titles:

- Cloud Support Engineer / Junior Cloud System Analyst / Junior Cloud Network Engineer

Area of Work / Cluster Name	Major Tasks	Competency Requirements	Units of Competency (UoCs) Number	Relevant Qualification for fulfilling Competency Requirements
System configuration, maintenance and implementation of cloud infrastructure	1. Responsible for system configuration, maintenance, and provisioning as per set parameters	▪ Perform system testing against user, technical and hosting requirements ▪ Verify and validate that the deployed / migrated software and the existing software are functioning properly	111160L4 111159L4	Obtain qualification via training programmes (QF Level 4)
	2. Deploy, document, implement, and manage the cloud-based network and client network infrastructure solutions based on specific project needs	▪ Prepare system operation documentation ▪ Install and configure client/server application	111200L4 111120L4	
	3. Assist in the resolution of complex technical problems, while providing appropriate communications to all involved business partners and related stakeholders	▪ Apply diagnostic and troubleshooting skills to solve hardware, software and networking related issues. ▪ Analyse the performance, latency and accessibility of systems ▪ Manage organization resources for implementation across multiple processing environment	111121L4 111130L4 111163L4	

Area of Work / Cluster Name	Major Tasks	Competency Requirements	Units of Competency (UoCs) Number	Relevant Qualification for fulfilling Competency Requirements
		▪ Provide support to users	107867L2	
Quality Assurance and information security for cloud infrastructure	4. Support the quality assurance and security compliance	▪ Understand general security and network security features on various types of platforms ▪ Support and implement information security practices and procedures ▪ Ensure information security procedures and guidelines support information security policies ▪ Manage the day-to-day operations of service delivery	111195L3 ITSWIS404A ITSWIS402A ITSWOS421A	(Continued) Obtain qualification via training programmes (QF Level 4)

Proposed Competency Requirements (Cloud Computing - Support Level)

Relevant Job Titles:

- Computer Operator / User Support Staff / Technical Support Staff (TSS) / Field Technician / Help Desk Operator

Area of Work / Cluster Name	Major Tasks	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 qualification via training programmes (QF Level 3) Or RPL Mechanism (QF Level 3 RPL Cluster: ITOS010L3)
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 qualification via training programmes (QF Level 3) Or RPL Mechanism (QF Level 3 RPL Cluster: ITOS011L3)
System Security Support	3. System Security Support	▪ Create and maintain user accounts on server ▪ Configure user access control on server ▪ Administer system security	107885L2 107886L3 107888L3	Obtain qualification via training programmes (QF Level 3) Or RPL Mechanism (QF Level 3 RPL Cluster: ITOS009L3)
Web Support	4. 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 qualification via training programmes (QF Level 3) Or RPL Mechanism (QF Level 3 RPL Cluster: ITOS013L3)

Area of Work / Cluster Name	Major Tasks	Competency Requirements	Units of Competency (UoCs) Number	Relevant Qualification for fulfilling Competency Requirements
Operation Support (Technical Support)	5. Operation Support	▪ Maintain inventories of equipment / software ▪ Restore system or file from backups ▪ Monitor server system status ▪ Provide help desk support ▪ Preform system backup ▪ Perform simple webpage update	107892L1 107897L2 107898L2 107899L2 107901L2 107908L2	Obtain qualification via training programmes (QF Level 2) Or RPL Mechanism (QF Level 2 RPL Cluster: ITOS002L2)

Unit of Competency

Functional Area: Core Skills

Title	Provide support to users
Code	107867L2
Range	This unit of competency applies to IT support personnel who are responsible for providing technical support to users. This UoC illustrates the most common competences to provide support to users for application in their daily duties at their work place.
Level	2
Credit	3
Competency	Performance Requirements 1. Knowledge to provide support to users • Possess good communication, listening and interpersonal skills • Possess skills required to perform troubleshooting, provide instructions systematically and remote problem solving • Possess good knowledge of the products which are being supported • Possess basic knowledge of organisation’s internal support record system and support/problem knowledge base systems 2. Provide support to users • Understand Service Level Agreement (SLA) set by the organisation or department • Identify the support and type of issues that users are experiencing by applying different skills, including but not limited to the following: • Calm users and stay calm: Many users seek help only as a last resort which mean they are frustrated and often annoyed. Always helps to calm users so that information can be gathered • Patience: users have wide range abilities. Hence, some users will require extra efforts to support • Attentive: it is important to pay attention to individual user interactions (watching the language/terms that they use todescribetheir problems), as sometimes cannot describe the issues with verbal words • Stay confident: to provide the impression that the problem is not serious and transfer the confidence to the user • Time management: knowing how long to spend on the issue or troubleshooting before escalate for assistance • Dynamic and resourceful: not every user’s issues are the same. Need to be resourceful for troubleshooting and finding solutions • Prepare the supporting plan to troubleshoot and provide solutions to the reported issue which may be either on premise or remotely • Perform before and after event procedure, including but not limited to the following: • Complete all the required documents in accordance with the organisation’s procedures, such as problem reports, etc. • Liaising with vendors for product information, parts, etc. • Liaising with service providers on purchased service • Coordinating with onsite engineers 3. Exhibit professionalism • Possess customer service oriented attitude • Apply industry best practices for user support and being up-to-date with technology trends including but not limited to: cloud computing, Internet of Things (IoT), virtualisation technologies, and mobile technologies

Unit of Competency

Functional Area: Core Skills

Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Communicate with users to effectively and efficiently to obtain required information on issues encountered by the user • Provide help to users effectively • Perform before and after support procedures effectively
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

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

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	Maintain inventories of equipment/software
Code	107892L1
Range	This unit of competency applies to IT support personnel who need to maintain inventories of the organisation equipment and software. One of their key tasks is knowing where equipment/software are and how many there are. Hence, well maintained inventory control systems, of any sort (manual or computerised system), will be most beneficial when providing maintenance to them. In this UoC the term inventory implies information records of equipment and/or software license own by the organisation. Information includes but not limited to: type of equipment/license, where they are being used, purchased date, etc.
Level	1
Credit	3
Competency	Performance Requirements 1. Knowledge for maintaining inventories of equipment/software • Possess basic reading, writing and interpretation skills • Possess well organised skills • Possess basic knowledge of the organisation inventory system • Possess good knowledge of organisation’s inventory guidelines and procedures 2. Maintain inventories of equipment/software • Create inventory list (or database) for different types of equipment and software, if it’s not already exist, such as: • Computer systems • Monitors • Word processing software license • Server license • For each inventory list, create a record for each purchased/delivered. For example the Computer System inventory list: record1 for the 1st received computer, record2 for 2nd received computer, etc. • For each record follow the organisation’s convention to collect and record required information, such as: • Reference/Identification number • Description • Purchased date • Supply details • Location of used • Proceed to marking reference number or adhering inventory label on the corresponding equipment • Periodically perform inventory check and update inventory list, in accordance with the organisation’s guidelines and procedures 3. Exhibit professionalism • Committed to ensure inventory records are well maintained to provide efficient reporting and support functions that conforms to organization standards
Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Explain the need for well-maintained inventory records of equipment • Follow the organisation’s guidelines and procedures to maintain various inventory lists that are used during operation support by service team
Remark	

Unit of Competency

Functional Area: System and Hardware Support

Title	Restore system or files from backups
Code	107897L2
Range	This unit of competency applies to support personnel who assist users to recover files from backup due to accidental loss or perform full system restore due to system corruption. In the context of this UoC, the term “files recovery” implies partial restore and “system restore” implies a full restore which is needed for a system rebuild. Backups are normally held on offline media created from full or partial backup that are performed regularly. Examples of backup media include but not limited to tape, USB/mobile disk, or USB memory stick.
Level	2
Credit	3
Competency	Performance Requirements 1. Knowledge for restoring system or files from backups: • Familiar with various backup and restore methodologies • Familiar with different system backup, such as: full backup, incremental backup and differential backup • Possess good knowledge of operating backup and restore application • Familiar with the organisation’s media labeling system for different generations of backups • Familiar with operating backup and recovery applications 2. Restore system or files from backups • Determine types of restoration from job request. Follow the organisation’s guidelines to confirm ownership of the restored file and/or authorisation for restore of files or system • Determine date for system restore or details related to the files to be restored, such as: • File name • Date and time • Destination of restore • Owner of the file • Locate and mount the backup media for system or files restore. Sequence of media mount may be required for restore of incremental or differential backups • Set the mounted media to be “read only” to avoid accidental deletion of backup items • Use suitable restoration application to verify that the mounted media is of correct date for system restore or that the located files matched the required restored files • Specify destination and initiate the restore process • Confirm successful restoration from restoration log or system message • Confirm successful restoration with user or supervisor • Perform temporary location cleanup, if necessary • Return all backup media to store for safe protection and complete documents of restoration work in accordance with the organisation procedures, such as log of restoration work, authorisation details, etc. 3. Exhibit professionalism • Be empathetic and exhibit willingness to help users restore lost or damage files from backup • Follow the organisation guidelines and procedures for restoring systems and file • Be aware of security guidelines and best practices in handling intellectual property

Unit of Competency

Functional Area: System and Hardware Support

Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Follow the organisation's policies and security procedures when restoring systems or files for users, including acquiring authorisation before restore of systems or files • Identify the restoration work details necessary for performing the restoration correctly • Operate the restoration application or facilities to locate and restore the requested files for the user
Remark	

Unit of Competency

Functional Area: System and Hardware Support

Title	Monitor server system status
Code	107898L2
Range	This unit of competency applies to IT support personnel who are responsible to monitor the organisation’s server status and take appropriate actions in accordance with organisation procedures. In an IT shop, large or small, there are a number of critical servers either dedicated or virtualised. These servers provide many services and are accessed by countless number of users. Are they functioning as they should be? Are there any unauthorized access? Have all the services started correctly? Are there messages from the servers that required human interaction? IT personnel will go through regular routine, daily or predefined schedule, to monitor server activities to ensure they are functioning and security protected. Where necessary taking corrective actions in response to system messages.
Level	2
Credit	3
Competency	Performance Requirements 1. Knowledge for monitoring server system status: • Possess good literacy skills • Possess good knowledge of different server operating system • Familiar with server monitoring and troubleshooting tools, including system logs, system diagnostic utilities and network monitoring tools • Familiar with the organisation’s server monitoring guidelines and procedures • Understand the organisation’s server security procedures and requirements • Familiarised with escalation procedures 2. Monitor server system status • Comprehend the organisation’s server support manual and procedures, server monitoring check list, • Set server monitoring triggers, alarms, and monitoring parameters in accordance with the organisation’s server monitoring guidelines and procedures • Follow the scheduled check list to perform the following checks: • Scan system services activities to verify all the required services are active, such as: network services, system services, messaging services, etc. • Study system event log for error or warning, such as system update failure, system rebooted abnormally, etc. • Study system security log for unusual activities, such as a user account tried to login many times, accounts locked out, etc. • Study the server performance monitoring tools to determine various system resource usage, such as CPU, memory, network, storage, etc. • Study application logs for errors and warnings, such as ftp and web server problems, etc. • Study virtual server logs to monitor all virtual clients systems are active, operating normally, virtual environment and resources are optimal assigned that does not affect its performance, security is protected, virtual devices are still connected, etc. • Evaluate monitored result. Report, perform appropriate actions, and/or escalate problems in accordance to the organisation’s guidelines and procedures • Backup monitoring and event logs for record keeping and/or evidence • Complete the necessary documents in accordance with the organisation standards and procedures 3. Exhibit professionalism • Always apply industry best practices and follow the organisation guidelines and procedures when performing monitoring of the organisation’s server

Functional Area: System and Hardware Support

Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Comply with the organisation’s server monitoring guidelines and procedures to monitor all events, performance, resources and security of servers • Evaluate monitored results and follow the organisation guidelines to take appropriate actions and enact escalation procedures when required
Remark	

Unit of Competency

Functional Area: System and Hardware Support

Title	Provide help desk support
Code	107899L2
Range	This unit of competency applies to support personnel who are responsible for providing front line help desk support. This is the first point of contact (telephone or face to face) for users seeking technical assistance or information. The duties of support personnel include but not limited to the following: handle customers enquires, perform problem analysis, provide resolution for simple problems, and create “Trouble Tickets (TT)” or problem log to record reported problem and solution.
Level	2
Credit	3
Competency	Performance Requirements 1. Knowledge to provide help desk support: • Possess good communication and interpersonal skills • Possess good troubleshooting skills and capable of providing systematic instructions for remote problem solving • Understand committed Service Level Agreement (SLA) standards • Possess basic knowledge of the organisation’s problem escalation procedures and guidelines • Possess basic knowledge of the organisation computer hardware, Operating System (OS), applications and network equipment 2. Provide help desk support • Greet the user politely and patiently listen to their reported issues and symptoms • Use appropriate questioning techniques to determine where/what the issues lie, such as: OS, application software, hardware, network connection, Web access, etc. • Refer to history problem log to determine if similar problems and solutions exist • Formulate a solution for user • If instant rectification is possible: • Explain rectification procedure to the user • Step by step explain what action the user needs to perform, giving details of what user can see on their system screen and system messages, if any • If on premise support is deemed necessary, inform the user that the issue will be escalated to next level of support and provide an indication of when the user will be contacted • Confirm solution is acceptable with user • Perform the necessary documents and create a Trouble Ticket/problem report to record the supported event in accordance with the help desk support procedure. Where necessary, coordinate with other colleagues, such as requesting site engineers to visit the user 3. Exhibit professionalism • Possess customer service oriented attitude ensuring customer is satisfied with the services provided • Always keep customer informed of actions and status of the rectification process • Follow organisation safety procedures when performing troubleshooting and/or reification of equipment

Unit of Competency

Functional Area: System and Hardware Support

Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Communicate with users at the correct technical language level • Understand the user's issue, performing first level simple troubleshooting/analysis and satisfactorily provided a solution/explaination to the customer • Complete the "after event" procedures in accordance with the organisation's procedures and guidelines
Remark	

Unit of Competency

Functional Area: System and Hardware Support

Title	Perform system backup
Code	107901L2
Range	This unit of competency applies to support personnel who are responsible for performing backups. System backup may be a full system backup, database backup or file backup performed in regular basis or ad-hoc basis. The support personnel follow a set of predefined procedures or directive from supervisor to ensure the correct generation of backup media is used and correctly labelled after the backup. Media can be tape, disk or any other removal storage.
Level	2
Credit	3
Competency	Performance Requirements 1. Knowledge on performing system backup: • Familiar with various backup methods and its advantages, such as “Full Backup”, “Differential backup” and “Incremental backup” • Familiar with and appreciate the needs of backup in multiple generations • Familiar with the advantages and disadvantages of different backup media • Possess the ability to: • operate backup software application • mount backup media • Grasp the importance of backups to an organization 2. Perform system backup • Comprehend the organisations’s backup procedures/instruction and clarify any unsure area with supervisor, if needed • Collect and identify backup media is the correct generation. • Prepare the media for backup, including: • Mount the media • Validate and ensure sufficient space available for backup • Ensure media is not write protected • Initiate backup from backup application • Verify completion and success of backup from application’s message or log • Perform post backup procedures, including: • Dismount media from backup device (if needed) • Label the media in accordance with the organisation guidelines • Store the media in accordance with the organisation procedures • Complete necessary administration documents, in accordance with the organisation procedures, to record details and the completion of backup 3. Exhibit professionalism • Comply with the data privacy and security laws • Ensure all backup are performed in accordance with the organisation standards that complied with any regulatory requirements, if any
Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Follow the organisation procedures to complete the backup (system, database, or files) as required The integrated outcome • Correctly select the appropriate media generation for backup • Correctly label and store the media in accordance with the organisation’s procedures
Remark	

Unit of Competency

Functional Area: Web Support

Title	Perform simple web page update
Code	107908L2
Range	This unit of competency applies to junior IT personnel who are responsible to maintain simple basic web pages of the organisation’s website. The IT personnel can use any web page editing tool or simply a text editor with HTML to maintain the basic web page which typically includes: static text, images, videos, links, etc.
Level	2
Credit	3
Competency	Performance Requirements 1. Knowledge to perform simple web page update • Possess basic principles of website design and maintenance • Possess good knowledge of web contents editing tools • Possess good knowledge of common web browsers • Possess basic knowledge of file transfer tools • Possess basic knowledge of web page testing • Possess in-depth knowledge of HTML • Possess good knowledge of the organisation documents standards and procedures 2. Perform simple web page update • Comprehend the web page enhancement requirements • Locate and obtain a recent copy of the concerned web page from backups or download from the web server • Obtain all the content materials to be used for updating the web page such as images, videos, links, etc. • Select the appropriate editing tool to maintain the web page, such as: text editor, Dreamweaver, Visual Studio, etc. • Edit the web page with the information as required, including but not limited to the following: • Add/remove text contents • Correct broken links or references • Insert new or delete old links or references • Perform headings, images and colour revision • Copy or upload the new version of the web page and other new contents to the web server, keeping the older version for rollback purpose • Test and confirm the changed web page are valid • Test the updated web page can function to all common web browsers • Perform after update procedures, including back up the new version of the web page, removing obsolete web contents from the web server, etc. • Complete documents of the updated web page that fulfills the organisation’s guideline and procedures 3. Exhibit professionalism • Always protect the interest and image of the organisation • Apply industry best practices and web technologies when maintaining website • Ensure web contents complied with Intellectual Property and copyright laws

Unit of Competency

Functional Area: Web Support

Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Correctly maintain the web page using appropriate editing tools that fulfil designed requirements • Complete all necessary testing that complied with the organisation's procedures to ensure the web page functions as designed • Complete all the after update procedures that complied with the organisation standards
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

Title	Build simple web site using content management systems
Code	107911L3
Range	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.
Level	3
Credit	3
Competency	Performance Requirements 1. Knowledge for building simple web site using content management systems • Possess good communication and interpersonal skills • Possess good knowledge of web hosting concept and sourcing of hosting facilities • Possess detail knowledge of implementing web CMS systems • Possess detail knowledge of operating and administering the organisation’s CMS • Possess basic knowledge of HTML • Possess some basic training skills 2. Build simple web site using content management systems • Work with supervisor and other stakeholders to identify the website technical requirements from, such as: ◦ Type and usage of web site (dynamic, static, Internet store, etc.) ◦ Performance required (response time) ◦ Size of storage ◦ Network speed • Identify suitable web CMS and web hosting company (unless for the organisation use, taking into various factors, including: ◦ Prices ◦ Backup service ◦ Facilities offered (storage, network bandwidth, CPU speed, etc.) • Prepare purchasing document, in accordance with organisation procurement procedures, and recommendation for supervisor approval • 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 • Download and perform remote installation web CMS on hosting server • Access administrative functions of web CMS to perform following tasks: ◦ Upload and install a template for the website ◦ Upload company logo and other media (pictures and video) contents for the home page ◦ Edit the home page with CMS editor • Test the web site with different web browsers to ensure compatibility • Create login accounts and provide tutorial sessions for web designers to use the CMS editor to create web pages on the web site 3. Exhibit professionalism • Be familiar with W3C web standards and ensure the CMS and web site are W3C compliant • Always look after the interest of the organisation when dealing with external parties

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 & Communications Technology Industry
Unit of Competency

1. Title	Perform Installation and configuration of internet server application
2. Code	111120L4
3. Range	This UoC involves carrying out installation and configuration of internet server application according to predefined requirements.
4. Level	4
5. Credit	6 (for reference only)
6. Competency	Performance Requirements 6.1 Knowledge in installation and configuration of internet server application, including ● networking and internet server ● common operating systems ● testing and troubleshooting internet server applications 6.2 Install and configure internet server application ● Prepare an installation plan for the internet server application requirements including but not limited to the following: ■ Identify what installation options are required from work order ■ Identify hardware, software, network and security requirements ■ Identify what data migration is required, if any ● Prepare for installation ■ acquire the server application installation media ■ familiarise with the server application installation instructions from vendor documents ■ acquire associated settings for the server application such as network confgiruations, firewall confgiruations, authorised access account settings ■ acquire all necessary technical manuals ■ perform server backup if necessary ■ install and configure network settings, middleware, database, if required ● Install and configure the server as required by the work order ■ configure security and access settings to allow client to connect ■ apply appropriate patches and updates ■ undertake restore or migration of data, if required ■ perform appropriate tests ● Perform post installation procedures ■ clean up work area and remove temporary work files and objects from the server ■ perform backup image of the server 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 6.3 Exhibit professionalism ● perform post installation procedures that in compliance with the organisation guidelines and procedure ● make reference to the industry best practices for installing server applications
7. 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 server application without any delay ● ensure the installation process is carried out efficiently without affecting other applications and/or services on the server ● perform post installation procedures that complied with the organisation guidelines and procedure
8. Remark	

Specification of Competency Standards for the Information & Communications Technology Industry

Unit of Competency

1. Title	Apply diagnostic and troubleshooting skills to solve hardware, software and networking related issues
2. Code	111121L4
3. Range	This UoC involves troubleshooting and identifying the causes of the problem in ICT systems.
4. Level	4
5. Credit	3 (for reference only)
6. Competency	Performance Requirements 6.1 Knowledge in hardware, software and networking aspects and diagnosis of hardware, software and networking aspects in ICT systems. 6.2 Troubleshooting across hardware, software and networking aspects in ICT systems ● comprehend the issues and symptoms of the issues from the problem report or from user and plan how to troubleshoot the issues. ● apply appropriate diagnostic tools and command set to obtain the status of the system. ● attempt to reproduce the issues that were reported and collect as much information as possible for problem analysis. ● When needed, consult colleagues, professionals and vendors ● formulate an action plan to implement the solutions to rectify the issues. 6.3 Exhibit professionalism ● take necessary measures to prevent or minimise data loss or service interruption during the diagnosis process. ● follow organisation safety procedures when handling any hardware or equipment during the troubleshooting process. ● follow organisation Standard Operating Procedures (SOPs) or guidelines when handling the troubleshooting process.
7. Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: ● apply proper diagnostic tools and system functions for problem identification. ● plan the troubleshoot work and systematically perform the troubleshooting to identify the issues or cause of issues. ● follow organisation procedures when handling any hardware or equipment during the troubleshooting process.
8. Remark	

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

1. Title	Define data governance policies and architecture principles
2. Code	111123L6
3. Range	This UoC involves defining the data governance policies and scope of data assets for the establishment of data architecture to support the development of organisational data being accurate, accessible, consistent and protected.
4. Level	6
5. Credit	3
6. Competency	Performance Requirements 6.1 Understand the data governance policies and scope of data throughout the data lifecycle ● Be able to: ■ Have knowledge of data governance policies (see Remark 1) and scope of data (see Remark 2) 6.2 Define the data governance policy for the establishment of data architecture to support the development of organisational data being accurate, accessible, consistent and protected ● Be able to: ■ define the processes to be implemented in your data governance initiative ■ define roles and assign responsibilities ■ initialize the data governance framework ■ define the required deliverables and organization structure for data governance 6.3 Review the data governance policy ● review the data governance policy such that the data asset are consistent and confident for the business decisions based on trustworthy data aligned with all the various purposes within the enterprise
7. Assessment Criteria	● The integrated outcome requirement of this UoC is the abilities to define the governance policy to make consistent and confident business decisions based on trustworthy data aligned with all the various purposes for the use of the data assets within the enterprise
8. Remark	1. The data governance policy will deal with the internal policies and external policies for data quality, access, security, privacy and usage, as well as roles and responsibilities for implementing those policies and monitoring compliance with them against organisational culture, types of business, ethics, regulatory, compliances, standards, etc. 2. The appropriate protection and security levels for different classifications of data within the scopes of data include (but not limited

	to) data ownerships, data custodians, data retention, data sharing, data archive and data disposal

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

1. Title	Define metrics to ensure that a technology architecture meets the business goals
2. Code	111127L5
3. Range	Define metrics to evaluate and analyse technology architectures to ensure that it can support the business goals and objectives.
4. Level	5
5. Credit	3 (for reference only)
6. Competency	Performance Requirements 6.1 Understand the principles of quality assurance ● articulate the needs for quality assurance to ensure that the resulting technology architecture really meets the required quality standards ● understand the quality assurance standards and measures provided by IT service providers 6.2 Understand the purposes of relevant metrics for quality assurance standards ● understand appropriate and measurable metrics to evaluate the ability of a technology architecture to meet the business goals and objectives (See Remark) 6.3 Define metrics for quality assurance standards ● keep updated of the business and technology changes ● observe the code of practices in trade ● update the developed software deployment or migration plan and contingency plan whenever necessary 6.4 Exhibit professional skills ● a formal checkpoint review of the architecture model and building blocks with stakeholders, validating that the business goals are met ● document all findings
7. Assessment Criteria	The integrated outcome requirements of this UoC is the ability to: ● validate that the business goals and other objectives of implementing the technology architecture are met. Please note that this may be a continuous exercise because of the ongoing changes of business requirements and technology options. This makes the definition of quality assurance standards and metrics a key to this activity.
8. Remark	An example of the metrics can be a key question list which is used to pose questions against the architecture model and service description

	portfolio to test its merit and completeness

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

1. Title	Develop the microservices architecture
2. Code	111128L5
3. Range	Develop a microservices architecture reference model from various viewpoints to align with the business requirements as well as requirements from higher level architecture
4. Level	5
5. Credit	3 (for reference only)
6. Competency	Performance Requirements 6.1 Review the benefits and challenges of a microservices architecture ● Be able to ■ understand the benefit of decomposing an application into microservices, such as modularity, scalability, integration, etc ■ understand the protocols that microservices communicate with each other ◆ Synchronous ◆ Asynchronous ◆ UI integration ■ address the challenges of embarking on a microservices architecture ◆ Complexity ◆ Lack of governance ◆ Latency ◆ Data integrity ◆ Versioning 6.2 Understand various microservices architecture reference models ● Be able to ■ understand the development processes for building a microservices architecture ■ identify the boundaries of the microservices ■ understand the strategy of decomposing and decoupling a monolithic application into a series of microservices 6.3 Develop the microservices architecture by evaluating business capabilities, and the software and hardware environment. ● Be able to ■ choose suitable hosting model for the computing resources ■ depict the microservices that enable reasoning about critical requirements and constrains all subsequent refinements. ■ conduct the evaluation and perform the analysis of the

	microservices
7. Assessment Criteria	The integrated outcome requirements of this UoC is the ability to develop a microservice architecture in alignment with the business capabilities, and software and hardware environment as well as the business requirements from higher level architecture
8. Remark	

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

1. Title	Analyse the performance, latency and accessibility of systems
2. Code	111130L4
3. Range	This UoC involves analysing the performance, latency and accessibility of computer systems across multiple processing environment in accordance with the organisation's guidelines and/or requirements.
4. Level	4
5. Credit	3 (For Reference Only)
6. Competency	Performance Requirements 6.1 Understand the attributes to measure the performance of computer systems across multiple processing environment, including but not limited to: ● Availability ● Extensibility ● Interoperability ● Maintainability ● Reliability 6.2 Understand the effect of latency and accessibility of computer systems across multiple processing environment, including but not limited to: ● Virtualization ● Distributed computing ● Data center Location ● Sensor and actuator network ● Streaming media ● Esports and online multiplayer games 6.3 Know the enhancement of accessibility and analyse the performance of computer systems across multiple processing environment to provide suitable strategies for the benefits of the organisation
7. Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: ● analyse the performance, latency and accessibility of computer systems across multiple processing environment for an organisation in accordance with its guidelines and/or requirements. ● provide suitable recommendations for the benefits of the organisation.
8. Remark	

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

1. Title	Define a system migration plan
2. Code	111155L6
3. Range	Define a system migration plan taking into account the business operations (including contingency plan) in the context of migrating systems
4. Level	6
5. Credit	3 (for reference only)
6. Competency	Performance Requirements 6.1 Understand the requirements in system migration ● Be able to ■ comprehend the organisational requirements, limitations and constraints on the system migration ■ identify all components of the system that need to be migrated ■ know the regulatory requirement such as audit trails or other compliance requirements ■ know the share responsibility model with IT service providers 6.2 Develop and define a system migration plan and a contingency plan ● Be able to ■ perform reviews of software requirements, hardware infrastructure, software architecture, components, interfaces and performance model ■ identify components that need to be updated ■ make suggestions on how to upgrade the system, for example, with the use of the latest technological developments ■ future-proofing the system by accounting for the adaptation of potential future technologies ■ list out the required deliverables upon migration ■ identify the critical success milestone and criteria in migration ■ formulate a system migration plan by integrating the known factors and also taking into account the available migration timeline ■ suggest an alternative contingency plan as a backup to cope with adverse cases ■ alert of associated personnel for potential downtime to minimise impact to the operation of the organisation 6.3 Update the migration plan ● Be able to

	■ stay on top to keep abreast of the pace of business and technology changes ■ observe the code of practices in trade ■ update the developed system migration plan and contingency plan whenever necessary 6.4 Define system migration plan in a professional manner ● Be able to ■ define a system migration plan ■ define the contingency plan of the migration exercise ■ minimise impact 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： ● devise and update a system migration plan and the related contingency plan for the migration exercise ● minimise impact to the organisation's operation
8. Remark	

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

1. Title	Perform risk assessment on system migration
2. Code	111157L6
3. Range	This UoC involves analysing the cloud deployment/migration plan by taking into account the in-house system confirmation and business operations
4. Level	6
5. Credit	6 (for reference only)
6. Competency	Performance Requirements 6.1 Understand the risk factors in software deployment or migration ● Be able to list out the general risk factors in software deployment or migration such as ■ tight schedule in deployment timeline ■ insufficient scale of suitable hardware for software deployment or migration ■ lack of network bandwidth for remote sites ■ no automatic tool available for large scale deployment or migration of software ■ incompatible of the existing architecture ■ unwanted latency after migration ■ lack of visibility and control ■ data loss/corruption during the migration process ■ security risk including but not limited to: ◆ compliance violations ◆ security breaches ◆ insecure APIs ◆ misconfiguration ◆ hijacking of accounts services ◆ insider threats 6.2 Perform risk assessment on software deployment and migration ● audit the legacy architecture/system and minimize the inconsistencies and interoperability problems on software deployment or migration exercise ● evaluate the impact of each risk factor on the software deployment or migration exercise ● consolidate the impacts from possible risk factors in qualitative and quantitative terms 6.3 Report the risk assessment to stakeholders ● rank the identified risk factors according to the severity to the

	business entity, such as ■ key benefits and security risks of Cloud Computing ■ obligations of Cloud service provider under the share responsibility model ● report the findings to stakeholders in good faith 6.4 Perform risk assessment on software deployment and migration in a professional manner ● formulate and execute a recovery/restore plan ● perform risk assessment on software deployment and migration in accordance with the organisation’s 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: ● analyse the cloud deployment / migration plan ● perform a risk assessment on cloud deployment / migration exercise.
8. Remark	

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

1. Title	Verify and validate that the deployed / migrated software and the existing software are functioning properly
2. Code	111159L4
3. Range	Verify and validate that the deployed/migrated software and the existing software are functioning properly in the context of deploying and migrating software
4. Level	4
5. Credit	6 (for reference only)
6. Competency	Performance Requirements 6.1 Understand the relationship between the deployed or migrated software with other systems ● Be able to ■ state the features of the newly deployed software ■ state which functionalities from the retired software were replaced by that from the migrated software ■ identify the position of the deployed or migrated software in the integrated environment within an organization 6.2 Perform verification and validation on the deployed or migrated software ● Be able to ■ draw up a verification and validation plan on the deployed or migrated software for subsequent verification and validation process ■ trace the recorded results from deployment or migration process and any other traceable reports to determine whether the software was implemented correctly and completely according to defined requirements such as those in the area of ◆ Performance ◆ Data security and integrity ◆ Interoperability with other system components 6.3 Ensure independent operation in verification and validation process ● Be able to ■ conduct additional tests to verify and testify that the deployed / migrated software and any existing software are functioning properly ■ walkthrough all steps in verification and validation plan ■ review documentary evidence received and fully document audit works ■ ensure audit documentations are properly retained by

	following the organisation’s / auditor’s guidelines 6.4 Verify and validate the deployed / migrated software and the existing software are functioning properly professionally ● Be able to verify and validate the deployed / migrated software and the existing software are functioning properly in accordance with organization’s guidelines as well as any (local and international) laws and regulatory requirements, if applicable
7. Assessment Criteria	The integrated outcome requirement of this UoC are the abilities to： ● confirm that the deployed or migrated software delivers its expected outcomes ● confirm that the deployed or migrated software and the existing software are functioning properly
8. Remark	

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

1. Title	Perform system testing against user, technical and hosting requirements
2. Code	111160L4
3. Range	Identify all elements of the system that need to be tested against user and system requirements, including data that should be used to fully test the system.
4. Level	4
5. Credit	3 (For Reference Only)
6. Competency	Performance Requirements 6.1 Have the knowledge to design and develop test plans and software/sensor simulator to facilitate different levels of testing ● Be able to: ■ identify the requirements of test plans ■ identify the requirements of software/sensor simulator, if applicable 6.2 Perform various levels of testing, which may involve the use of a software/sensor simulator ● Be able to: ■ design and develop software/sensor simulator, if applicable, to facilitate different levels of testing ■ perform the required testing activities of various levels of testing according to the corresponding test plans 6.3 Perform all testing activities in a professional manner ● Be able to ■ perform the testing activities of various levels of testing in an efficient and effective manner ■ ensure that all such testing activities are complied with the corresponding test plans and are in accordance with the organisation’s 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: ● develop appropriate software/sensor simulators, if necessary, for testing purposes; ● perform various levels of testing; and ● document all testing activities in test reports.
8. Remark	Various levels of testing include unit testing, integration testing, system testing – functional testing and performance testing, and user-acceptance testing.

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

1. Title	Define user requirements
2. Code	111162L4
3. Range	This UoC involves defining user requirements of IT application and communicating with stakeholders to produce a user requirement document
4. Level	4
5. Credit	6 (for reference only)
6. Competency	Performance Requirements 6.1 Know the stakeholders and information needed to be conveyed ● understand the relationship of business requirements, user requirements and system requirements for defining an IT application development project ● identify the stakeholders who will be the users of the IT application to be developed ● collect profile of stakeholders, whenever possible, to preliminarily identify what the users do with the IT application or what activities the users must be able to perform ● understand any constraints on the delivery of information such as time and location etc. 6.2 Consolidate information for delivery ● collect relevant data and compose a draft appropriate to the communication assignment ● explain the use of special terms and short forms ● bridge the gap between technical and non-technical people by communicating technical terms in generic terms ● seek recommendation or approval from management before release of information where necessary 6.3 Exhibit professionalism in the user requirement document ● follow the organisation’s style and format to prepare the user requirement document ● produce accurate and concise the user requirement document
7. Assessment Criteria	The integrated outcome requirement of this UoC are the abilities to： ● understand and identify the needs of stakeholders for an IT application design project ● communicate technical information to non-technical people effectively ● Produce accurate and concise user requirement document
8. Remark	

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

1. Title	Manage organisation resources for implementation across multiple processing environment
2. Code	111163L4
3. Range	This UoC involves managing organisation computing resources devoted to multiple platform processing environment for the benefits of the organisation.
4. Level	4
5. Credit	3 (for reference only)
6. Competency	Performance Requirements 6.1 Understand the key principles of managing computing resources ● Be able to know the principles of managing the computing resources across multiple processing environment ■ Automation ■ Identity and Access Management ■ Continuous integration and development ■ Optimisation of course costs and consumption 6.2 Understand the available resources of the organisation ● Be able to ■ list the on-premise computing resources of the organization accurately ■ understand the computing resources required for the future business development 6.3 Define the computing resources management plan in accordance with the IT strategies ● Be able to ■ manage on-premise computing resources effectively ■ choose the suitable on-demand service models across multiple processing environment, such as ◆ Infrastructure as a service (IaaS) ◆ Platform as a service (PaaS) ◆ Software as a service (SaaS) ◆ Function-as-a-Service (FaaS) 6.4 Formulate plans to manage organisation computing resources for the benefits of the organisation ● Be able to formulate plans for managing the computing resources on-premises and on multiple processing environment according to the business requirements

7. Assessment Criteria	The integrated outcome requirements of this UoC is the ability to manage both on-premises computing resources and resources on multiple processing environment for the benefits of the organisation.
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	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	Formulate data security and consent policy for emerging technologies
2. Code	111186L5
3. Range	This UoC involves formulating data security and consenting policy for an organisation to adopt emerging technologies for supporting its business strategies
4. Level	5
5. Credit	3 (for reference only)
6. Competency	Performance Requirements 6.1 Know of the data security principles for emerging technologies (including but not limited to) ■ Accountability ■ Accuracy ■ Integrity and confidentiality ■ Purpose limitation 6.2 Know of regulations associated with data security and consent policy ● Knowledge of relevant security regulations (including but not limited to) ■ Personal Data (Privacy) Ordinance ■ European Union's General Protection Regulation (GDPR) ● Knowledge of roles of regulations in the digital society ● Knowledge of legal and economic perspectives underpinning data protection regulations 6.3 Formulate data security and consent policy ● Clearly define the data ownership and authority within the organization ● Identify the potential risks from improper use of data ● Select and adopt appropriate tools for the policy execution ● Ensure the policy to confirm to the relevant security and consent regulations ● Setup staff training direction to ensure that the staff could comply with the policy
7. Assessment Criteria	The integrated outcome requirements of this UoC is the ability to formulate data security and consent policy for an organisation to adopt emerging technologies with profound considerations of data security, and relevant consent regulations
8. Remark	

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

1. Title	Understand general security and network security features on various types of platforms to carry out network security assessment
2. Code	111195L3
3. Range	This UoC involves a good understanding the latest security challenges and opportunities presented by various platforms in order to identify the associated risks preliminarily in network security assessment.
4. Level	3
5. Credit	3 (for reference only)
6. Competency	Performance Requirements 6.1 Know the general security and network security features ● Understand different types of network security devices and tools (including but not limited to) ■ Access control ■ Antivirus ■ Application security ■ Data loss prevention ■ Email security ■ Firewalls ■ Mobile device security ■ Network segmentation ■ Security information and event management ■ Web security ● Understand the general concepts of network security ■ Confidentiality ■ Integrity ■ availability 6.2 Follow instructions/guidelines to ● carry out trouble shooting of security and network problems ● respond to all system and/or network security breaches ● carry out testing and identifying network and system vulnerabilities 6.3 Keep updated of the development of network security ● changes of local and international industry trends and requirements ● availability of new security devices and tools
7. Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to： ● understand different types of principles and devices of network security ● follow instructions/guidelines to perform network security assessment tasks

8. Remark	

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

1. Title	Conduct solicitation process in project outsourcing
2. Code	111196L5
3. Range	This UoC involves preparing and initiating the tender procedure for outsourcing parts of or the whole project.
4. Level	5
5. Credit	6 (for reference only)
6. Competency	Performance Requirements 6.1 Understand the outsourcing requirements ● Understand the organisation policies on outsourcing work ● Understand the project requirements and goals ● Aware of the technological skills needed for the completion of the project ● Have a rough idea of the budget ● Define a set of selection criteria 6.2 Awareness of the market condition ● Identify appropriate prospective bidders who are capable of providing the services ● Identify and collect information on services available in the market ● Aware of the reputation of different potential bidders 6.3 Prepare procurement documents ● Prepare all internal and external documents that are related to the solicitation process, for example: ■ invitation for Bid (IFB) ■ request for Proposal (RFP) ■ request for Quotation (RFQ) ■ initiation for Negotiation ■ contractor Initial Response 6.4 Invite or notify potential bidders and conduct bidder’s conference ● Send invitations to identified potential bidders ● Place advertisements to attract more potential bidders ● Establish key principles for conducting a bidder’s conference and clarify bidder’s concerns 6.5 Proposals collection and tender board formulation ● Receive tenders following guidelines ● Identify suitable members and invite them to be members of the tender board for the tender evaluation process

	6.6 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： ● develop effective procurement documents and procedures for the tender bidders to submit bids/quotations ● formulate a tender board with suitable members for the tender evaluation process ● carry out the solicitation process in accordance with organisation guidelines
8. Remark	

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

1. Title	Conduct solicitation planning
2. Code	111197L5
3. Range	This UoC involves preparing and specifying tender details for an organisation to outsource a particular project (whole or some of its part)
4. Level	5
5. Credit	3
6. Competency	Performance Requirements 6.1 Have knowledge in the market condition ● Be able to collect information about the products and services available in the marketplace 6.2 Understand the procurement cycle for outsourcing a particular project (whole or some of its part) ● Be able to understand the outsourcing activities for a procurement cycle 6.3 Prepare complete procurement documents ● Be able to: ■ design structured procurement documents that are used to solicit proposals from prospective sellers such as ◆ invitation for Bid (IFB) ◆ request for Proposal (RFP) ◆ request for Quotation (RFQ) ◆ initiation for Negotiation ◆ contractor Initial Response ■ ensure the documents can facilitate accurate and complete responses from prospective sellers as well as rigorous enough to ensure consistent, comparable but flexible responses to allow sellers to make suggestions for better ways in achieving the requirements 6.4 Be able to define evaluation criteria for rating or scoring proposals including the bidders' ● background ● financial capability ● past track record ● technical knowledge/skill ● resources availability 6.5 Form a tender board ● Be able to formulate the tender board with suitable members for

	the tender evaluation process
7. Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: ● develop effective procurement documents for the tender bidders submitting bid/quotation; and ● set up an accurate evaluation process for rating and scoring the submitted bids.
8. Remark	

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

1. Title	Analyse the available solutions from IT service providers
2. Code	111199L4
3. Range	This UoC involves analysing solutions from external IT service providers that fit most to the organisation's business goals
4. Level	4
5. Credit	3 (for reference only)
6. Competency	Performance Requirements 6.1 Knowledge in evaluation criteria of external IT service providers ● Technical expertise ● Domain expertise ● Business maturity Evaluation criteria of external IT service providers can also be divided into various sub-criteria. (See Remark 1) 6.2 Rank the proposals according to the criteria as listed in the procurement management plan 6.3 Make preparation for drafting the service agreement with the successful bidder ● Apply appropriate methods to identify service agreement concerns: ■ project warranties ■ liabilities ■ indemnity ■ insurance clause-related activities ● Make negotiation with the external service providers according to the rank sequence ● clarify any unclear points in the received proposal from the external service providers and negotiate with them on the terms and conditions according to relevant local / international laws ● reach consensus on the structure and requirements of the service agreement with the successful bidder prior to the signing of the agreement (Remark 2)
7. Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: ● apply appropriate criteria to evaluate proposals from external IT service providers ● make a fair selection for a successfully bidder and reach consensus with the successful bidder on the important terms and conditions for drafting the service agreement.
8. Remark	1. The evaluation sub-criteria are: ● Service / Product Value Creation / Provision ■ Service / Product Portfolio: Service scope including the

	completeness of the portfolio or the skill set. ■ Service / Product Experience: Service availability and service experience from a customer perspective. Maturity of the offer. ■ Integration: Interoperability of Technologies with one another or the skills to integrate them. ■ Economic factors: Price transparency and the quality of the business model, not the prices themselves. For service providers, nearshore concepts or skills that deliver low-cost architectures have also been evaluated. ■ Disruption potential: Recognition of the availability of highly innovative approaches ● Vendor Performance ■ Strategy: Strategy and market understanding. Does technology fit the company strategy? ■ Footprint: Competitive strength and market presence in terms of customers, reach, visibility and go-to-market. ■ Ecosystem: For IT service providers, the number of development service providers who are familiar with their technologies is critical. On the other hand, we evaluate the number of technology suppliers that are listed by Development Service Providers under Partners and Skills. Active involvement in open source communities is also a plus. ■ Customer Experience: Availability of information and training for technology providers. Local availability of employees for service providers. ■ Agility: Speed and innovation strength of the providers, assessed in terms of their ability to grasp market trends quickly and, if necessary, develop them with an innovation budget. 2. Subjects covered generally include, but not limited to, responsibilities and authorities, applicable terms and law, technical and business management approaches, contract financing and price.

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

1. Title	Prepare system operation documentation
2. Code	111200L4
3. Range	Prepare technical and user documentation describing how the system works for third party management. Documentation should reflect maintenance and update processes to ensure integrity the deployment.
4. Level	4
5. Credit	3 (For Reference Only)
6. Competency	Performance Requirements 6.1 Understand system requirements ● Be able to: ■ identify system operation issues, i.e. system installation/update and deployment, day-to-day technical operations, server or software application failure and maintenance, etc. ■ comprehend the workflow as stated in the system operation plan according to technical and user requirements 6.2 Prepare the operation documentation containing information that will aid system administrators to understand the functions and capabilities of your information technology systems, applications, and components ● Be able to: ■ describe the user typical processes and operation procedures as required by the needs of the technical and user requirements ■ provide standards on document to help with consistency and avoid potential pitfalls 6.3 Check the consistence and completeness of the documentation ● Be able to: ■ comply with corporate policy in documentation standards ■ review developed templates and guidelines to ensure their consistence in format and their completeness meet with system requirements ■ issue the developed templates and guidelines to stakeholders for review and feedback ■ incorporate feedback from stakeholders and management to finalise the system documentation standards
7. Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: ● establish system report and documentation standard and ensure consistency and completeness in the operation documentation ● enhance efficiency of system operation, support, maintenance and system training, etc.

8. Remark	

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

1. Title	Formulate business strategies and policies
2. Code	111201L6
3. Range	Formulate the business strategies and policies for an organisation in alignment with its approved vision and mission statements by considering the potential impacts and implications of both current and emerging technologies
4. Level	6
5. Credit	6 (for reference only)
6. Competency	Performance Requirements 6.1 Understand business objectives and envisioned future of an organisation ● Be able to ■ articulate the core values and purpose of an organisation ■ articulate the current trends of business and the envisioned future of an organisation 6.2 Understand issues related to both business and IT perspectives of the industry ● Be able to ■ understand the issues related to both business and IT perspectives of the industry ■ have insights of technology trends and viability of technology products under market forces ■ understand the potential impacts and implications of current and new technologies in the fields related to the organisation ■ think of possible ways to utilise new technologies in the organisation operation and marking strategy. 6.3 Understand the current development trends of a business ● Be able to summarise the business trends related to the organisation ● Aware of the business profile and positioning of the organisation ● Understand and state up to date with the business field related to the organisation 6.4 Understand the ICT applications related to a business ● Be able to summarise the ICT applications related to the operational aspect of the organisation ● Consider and make suggestions on updating current or adopting new technologies to enhance the operation and governance aspect of the organisation

	6.5 Analyse the strengths, weaknesses, opportunities and threats (SWOT) of an organisation ● Be able to perform a SWOT analysis for an organisation to develop business strategies and policies that bring reasonable and acceptable return of investment (ROI) 6.6 Formulate strategies and policies for the sustainability of the business ● Be able to ■ formulate the strategies and policies for the long-term sustainability of the business taking into consideration Business-IT alignment and enablement ■ formulate partnership/alliance strategies with external partners like vendors/suppliers, investors, distributors to win the market ■ carry out the above in accordance with the organisation’s business goals, objectives, policies and guidelines as well as any (local and international) laws and regulatory requirements, where applicable 6.7 Formulate ideas where IT can help the growth of the business ● Be able to identify and think of ways to update and implement technologies that could strengthen the operational goal and governance of the organisation
7. Assessment Criteria	The integrated requirements of this UoC are the abilities to： ● formulate business strategies and policies for an organisation in alignment with its approved vision and mission statements to support its sustainable development ● suggest updates to current technologies and adaptation of new technologies that could assist the development and governance of the organisation
8. Remark	Some examples of emerging ICT technologies are: ● Artificial intelligence and machine learning ● Cloud computing ● Internet of things ● Security and automation

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

1. Title	Identify and evaluate information technologies that support the objectives of an organisation
2. Code	111202L6
3. Range	This UoC involves applying analysis methods to identify and evaluate the information technologies that fit most to the organisation's business processes
4. Level	6
5. Credit	3 (for reference only)
6. Competency	Performance Requirements 6.1 Understand the organisation's objectives ● comprehend the organisation's vision, mission, objectives, goals and plans ● seek clarification on the above from relevant people, if necessary ● understand the implications of the organisation's objectives on the application of emerging technologies 6.2 Have broad knowledge of the information technologies applicable to the organisation's industry ● understand the emerging technologies landscape, including but not limited to: ■ Artificial intelligence and machine learning ■ Cloud computing ■ Internet of things ■ Security and automation ● understand the applicability, advantages and disadvantages, constraints and limitations of various information technologies available for the specific industry of the organization ● evaluate the opportunities and threats of the emerging technologies ● Understand the shared responsibility model with IT service providers, if applicable 6.3 Identify and evaluate information technologies that support the organisation's objectives with a high degree of expertise and professionalism ● identify and evaluate the appropriate information technologies for the organisation using standard guidelines and methodologies ● consider and evaluate the appropriateness of managed or outsourcing services. ● make appropriate references to industry sources, such as vendors

	and their customers, experts and consultants in the industry, etc.
7. Assessment Criteria	The integrated outcome requirement of this UoC is the ability to ensure that the information technologies identified and evaluated are the most appropriate to support the organisation’s objectives.
8. Remark	

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

1. Title	Maintain the portfolio management with different stakeholders
2. Code	111203L6
3. Range	Maintain the portfolio management with different stakeholders in the context of relationship management in an organisation to achieve its business goals and objective.
4. Level	6
5. Credit	3 (for reference only)
6. Competency	Performance Requirements 6.1 Understand the interests of different stakeholders ● identify the roles of different stakeholders (internal/external, upstream/downstream etc.) (Remark) ● assess needs and interests of different stakeholders (such as customers, colleagues, vendors/suppliers, and industry peers) 6.2 Communicate effectively and efficiently with various types of stakeholders ● identify the difficulties faced by different stakeholders and their bottom lines ● know how to stimulate or motivate the stakeholders 6.3 Understand the emerging technologies associated with portfolio management ● know the value of emerging technologies ● aware the relevant regulations and risks related to the emerging technologies 6.4 Maintain a professional relationship with various stakeholders ● plan engagement strategy and communication plan with various stakeholders ● manage and maintain the portfolio and relationship with stakeholders in order to establish mutual respect and trust
7. Assessment Criteria	The integrated requirement of this UoC is the ability to manage and maintain the portfolio and relationship with stakeholders for an organisation so as to achieve the organisation’s business goals and objectives while upholding mutual interests and establishing mutual respect and trust.
8. Remark	Stakeholders may include as customers, colleagues, vendors/suppliers, and industry peers etc.

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	Review the ethical and social issues for IT applications
2. Code	111208L6
3. Range	This UoC involves reviewing/addressing the social, environmental, political and legal challenges related to the emergence and convergence of information and communication technologies from the point of view of morality and ethics.
4. Level	6
5. Credit	3 (for reference only)
6. Competency	Performance Requirements 6.1 Understand the moral and ethical dimensions for IT applications ● identify and understand the major moral and ethical dimensions that tie together ethical, social, and political issues in IT applications including ■ Information rights and obligations ■ Property rights and obligations ■ Accountability and control ■ Application/system quality ■ Culture and lifestyle: economic disparity, equality and ethnicity on rights ● understand the impacts from technology advancement on individual and society such as data collection and analysis, privacy invasion etc. 6.2 Review the ethical and social issues for an organisation ● review the IT applications and/or processes within the organization from the point of view of morality and ethics ● identify and properly record any shortfalls relevant to moral and ethical considerations 6.3 Exhibit Professionalism ● always look after the interest of the organisation as well as customers.
7. Assessment Criteria	The integrated outcome requirements of this UoC is the ability to review the social, environmental, political and legal challenges related to IT applications/systems to support organisation’s business strategies from the point of view of morality and ethics
8. Remark	

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

1. Title	Establish a business continuity planning strategy
2. Code	111209L5
3. Range	Determines the competencies for defining cloud computing application continuity and recovery policies
4. Level	5
5. Credit	3 (for reference only)
6. Competency	Performance Requirements 6.1 understand the value of BCP in business operation; including reducing financial and operational impacts and ensuring the survivability of the corporation under different scenarios 6.2 Obtain executive support in BCP ● articulate the importance of BCP to an organisation's business upon unexpected interruption ● appreciate how the development and application of emerging technologies support business continuity ■ provide regular backups and easy failover ■ reduces downtime ■ reduce impact from cyber attacks ■ reduce the cost of maintaining a costly physical mirror site ■ eliminate the software synchronization ● obtain senior management commitment and full support on the execution of BCP in the organisation 6.3 Build business continuity model ● participate in the enterprise risk management process development cycle for building a BCP ● establish the strategy for the BCP based on business requirements, risk management model and regulation requirements ● define the roles and responsibilities of each individual / business unit for BCP execution 6.4 Define performance indicators ● develop models from different Business Impact Analysis methodologies ● understand and define the Mission Critical Business processes, Recovery Time Objectives (RTO), Recovery Point Objectives (RPO), and Acceptable Exposure to Loss according to business requirements

	● understand how the IT system will continue if on premise goes down but the cloud platform is still running, and vice versa, if applicable
7. Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to ● develop and obtain approval of a BCP strategy by obtaining senior management support ● building business continuity model
8. Remark	

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

1. Title	Formulate IT plans
2. Code	111210L5
3. Range	Formulate IT plans to illustrate the IT business model
4. Level	5
5. Credit	6 (for reference only)
6. Competency	Performance Requirements 6.1 Have good knowledge of IT business plans ● Be able to ■ understand the importance of documenting an IT business plan ■ understand the structure of an IT business plan 6.2 Develop the plans according to the objectives of the organisation ● Be able to ■ identify the IT business models of the organisation ■ identify the prioritised objectives for the whole organisation to achieve ■ develop the plan to fit the models and objectives above ■ account for new technologies and the potential adaption of them to enhance IT plans 6.3 Formulate IT business plans ● Be able to formulate IT plans, such as (but not limited to) the following: ■ hardware and software deployment and updates ■ software development and maintenance ■ procurement ■ IT outsourcing ■ IT services ■ IT infrastructure remodelling (e.g. replacing on-site network/storage with cloud services) ● Identify new technologies that are aligned to the organisation's goals and integrate them into IT plans for the benefit of the organisation 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 ● Stay up to date with the new developments related to the IT industry and the organisation's industry

7. Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to： ● formulate detailed IT business plans for the benefit of the organisation. ● refine IT business plans to implement technological updates that align with the organisation’s goals
8. Remark	

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

1. Title	Project the potential costs, benefits and ROI of IT project
2. Code	111211L5
3. Range	This UoC involves preparing and assembling a preliminary cost model so that an IT project can be completed within an approved budget and achieve the target Return On Investment (ROI)
4. Level	5
5. Credit	3 (for reference only)
6. Competency	Performance Requirements 6.1 Understand the budget planning of IT project ● understand the structure of an IT budget plan ● identify the existing available resources of the company ● identify the resources requirements of the IT business plan ● compute the cost of extra resources to acquire for budgeting ● conduct amortization of the current resources and factor the cost into the budget 6.2 Review the existing business strategies and policies against the business trends and business performance of the organisation ● examine the business performance against the identified performance indicators of the organisation ● analyse the effectiveness of the existing business strategies and policies in achieving business performance and matching with the business trends ● perform a SWOT analysis for an organisation to develop business strategies and policies that bring reasonable and acceptable Return of Investment (ROI) 6.3 Formulate an IT budget plan ● analyse the resource requirement above according to the IT plans ● develop and present a coherent budget plan according to industry standards ● regularly review the budget plan in accordance with the organisation's business goals as well as compliance requirements, and make adjustment whenever appropriate
7. Assessment Criteria	The integrated outcome requirement of this UoC is the ability to prepare a coherent budget plan according to IT business models and IT plans of the organisation
8. Remark	

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

1. Title	Ensure operable application integration architecture is in place	
2. Code	ITSWAR516A	
3. Range	Evaluate and define requirements for any necessary application monitoring and audit functions, and implement these functions on the adopted application integration architecture [Architecture – Application Integration Architecture]	
4. Level	5	
5. Credit	1	
6. Competency		Performance Requirement
	6.1 Establish application auditing requirements	Be able to ▪ define and establish application auditing requirements and checkpoints based on the adopted application integration architecture ▪ incorporate defined requirements and checkpoints into development methodology
	6.2 Create application audit functions	Be able to ▪ create quality assurance and audit functions and procedures to ensure the application integration architecture is of high quality ▪ incorporate those defined procedures into relevant documents such as development methodology
	6.3 Implement the audit functions	Be able to ▪ operate the application quality assurance and audit functions ▪ evaluate the outcomes of the quality assurance and audit functions against the relevant requirements
7. Assessment Criteria	The integrated outcome requirements of this UoCs are the abilities to ensure that application integration architecture is executable, manageable and auditable via setting up and implementing audit functions into the adopted application integration architecture.	
Remark	Application audit includes application monitor as it checks the operation of application integration against the requirements of the adopted application integration architecture.	

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

1. Title	Manage application integration architecture life cycle
2. Code	ITSWAR517A
3. Range	Define, manage and maintain resources to upkeep application in integration architecture in the most current status. [Architecture – Application Integration Architecture]
4. Level	5
5. Credit	1
6. Competency	Performance Requirement 6.1 Understand the life cycle concept of application integration — Be able to understand and document the life cycle of application integration including the relationships with other architecture models 6.2 Define a life cycle management policy — Be able to define a life cycle management policy including maintenance and change procedures of the adopted application integration architecture 6.3 Identify the resource requirements to meet the life cycle management policy — Be able to identify the resource requirements in need to review, maintain and change the life cycle of the application integration architecture 6.4 Maintain the life cycle management policy — Be able to utilize available resources to perform life cycle management of the application integration architecture work to ensure that the adopted architecture is ▪ correctly reflecting the current and future needs of the organisation ▪ in-line with the technology advancement and availability of such technologies from the industry
7. Assessment Criteria	The integrated outcome requirements of this UoCs are the abilities to ensure application integration architecture is properly managed and maintained.
Remark	

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

1. Title	Lead and motivate a team
2. Code	ITSWGS604A
3. Range	Lead and motivate a team in the context of managing and leading an organisation [Generic Skills – Management and Leadership – Personal Attribute]
4. Level	6
5. Credit	6
6. Competency	Performance Requirement 6.1 Have knowledge of the theories and techniques of leading and motivating a team Be able to ▪ understand the specific and unique needs of a team ▪ understand the various theories and techniques available for leading and motivating a team 6.2 Apply suitable skills in leading and motivating a team Be able to ▪ analyse and diagnose the specific and unique needs of a team, referencing appropriate theories and/or methodologies ▪ reference suitable sources to assist in the analysis and diagnosis ▪ steer and align team efforts with organisational objectives ▪ motivate team members to share knowledge and experience 6.3 Lead and motivate a team with a high degree of expertise and professionalism Be able to ▪ gain the respect and trust of the team members ▪ adjust leadership and motivational skills to cater to the different situations ▪ encourage full participation in meeting social responsibilities as well as quality performance ▪ lead the team to achieve results to the best of its capabilities and potentials
7. Assessment Criteria	The integrated outcome requirements of this UoCs are the abilities to: (i) demonstrate effective leadership in a team situation; (ii) motivate the team to a high spirit towards achieving certain goals; and (iii) lead a team to achieve excellent results that are aligned with organizational objectives.
Remark	

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

1. Title	Delegate responsibilities	
2. Code	ITSWGS606A	
3. Range	Delegate responsibilities in the context of managing and leading an organisation [Generic Skills - Management and Leadership – Personal Attribute]	
4. Level	6	
5. Credit	3	
6. Competency		Performance Requirement
	6.1 Have knowledge of the theories and techniques of delegation	Be able to ▪ understand the specific strengths and weaknesses of each staff ▪ understand the needs for delegation ▪ understand the various theories and techniques available for delegation of responsibilities
	6.2 Apply suitable skills in delegating responsibilities	Be able to ▪ analyse the strengths and weaknesses of staff ▪ delegate responsibilities to staff in accordance to their strengths and abilities ▪ clarify the understanding of staff on their responsibilities
	6.3 Delegate responsibilities to staff with a high degree of expertise and professionalism	Be able to ▪ delegate responsibilities to staff in a clear, effective and unambiguous manner ▪ exploit the full potential of staff in the delegation, and develop staff to the best of their capabilities and potentials ▪ achieve the best synergy among staff in the delegation
7. Assessment Criteria	The integrated outcome requirement of this UoCs are the abilities to (i) delegate responsibilities to suitable staff; (ii) develop staff potentials via proper job / task allocations; and (iii) exploit staff's full potentials via proper job / task allocations.	
Remark		

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

1. Title	Manage changes
2. Code	ITSWGS613A
3. Range	Manage changes within the organization [Generic Skills - Change Management]
4. Level	6
5. Credit	5
6. Competency	Performance Requirement 6.1 Understand change — Be able to ▪ understand the importance and need for changes ▪ understand the implications of changes 6.2 Cope with changes positively — Be able to ▪ identify if a change has occurred ▪ evaluate the impacts resulting from the change ▪ manage the change ▪ document the change 6.3 Grasp opportunities for improvement — Be able to ▪ minimize negative impacts resulting from the change ▪ leverage on the change to enjoy positive outcomes which would not have been obtained if the change had not existed
7. Assessment Criteria	The integrated outcome requirements of this UoCs are the abilities to: (i) cope with changes positively; and (ii) grasp opportunities resulting from changes for improvement.
Remark	

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

1. Title	Establish a business case for an IT investment
2. Code	ITSWGS617A
3. Range	Establish a business case for an IT investment for the organization including the assessment criteria [Generic Skills – Financial Management]
4. Level	6
5. Credit	11
6. Competency	Performance Requirement 6.1 Have good mastery on basic investment concepts — Be able to ▪ comprehend qualitative finance and investment concepts ▪ master basic quantitative finance techniques and ratios 6.2 Establish business cases — Be able to ▪ identify the development as either an infrastructure groundwork or application development ▪ understand the importance / benefits of IT development toward organizational objectives ▪ develop the storyline for the business case 6.3 Develop assessment criteria — Be able to ▪ list the qualitative benefits to the organization ▪ quantify the benefits wherever possible ▪ establish baseline ratios for assessment
7. Assessment Criteria	The integrated outcome requirements of this UoCs are the abilities to: (i) establish the business case for the software/system development; and (ii) develop assessment criteria and their baselines.
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	Report significant changes in risks	
2. Code	ITSWIS401A	
3. Range	Report significant changes in information security risks to appropriate levels of management of an organisation on both a periodic and event-driven basis [Information Security – Risk Management]	
4. Level	4	
5. Credit	1	
6. Competency		Performance Requirement
	6.1 Understand risk analysis methods and techniques	Be able to apply risk analysis methods and techniques to assess changes in risks
	6.2 Manage and report status of identified risks	Be able to manage and report significant changes in risks to appropriate levels of management on a periodic and event-driven basis according to the organisation’s policies and guidelines and applicable laws
7. Assessment Criteria	The integrated outcome requirements of this UoCs are the abilities to manage and report significant changes in risks to appropriate levels of management on a periodic and event-driven basis according to the organisation’s policies and guidelines and applicable laws.	
Remark	This UoCs assumes competencies as described in ITSWIS605A	

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	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	Manage the day-to-day operations of service delivery	
2. Code	ITSWOS421A	
3. Range	Manage the day-to-day operations of service delivery in the context of performing service level management services for an organisation [Operations and Support – Service Level Management]	
4. Level	4	
5. Credit	3	
6. Competency		Performance Requirement
	6.1 Understand the terms and conditions in service level agreement (SLA)	Be able to ▪ identify service level management customers and supportive service suppliers ▪ recognize that the SLA being a binding document primarily as an interface with the customers about service details contained in the operational level agreement (OLA) and underpinning contracts ▪ comprehend the terms and conditions in the SLA ▪ relate operating and support services to customer activities and the corresponding clauses in the SLA
	6.2 Ensure the currency and comprehensiveness of the SLA, OLA and underpinning contracts	Be able to ▪ control the release of SLA, OLA and underpinning contracts by proper change management procedures ▪ communicate the existence of the new SLA amongst the service desk and other support groups with details of when they become operational
	6.3 Produce service reports and circulate to customers	Be able to ▪ incorporate details of performance details against all SLA targets, together with any trends or specific actions being undertaken to improve service quality ▪ interpret trends of the actual service level performance and performance indicators ▪ estimate the resources required to produce and verify reports ▪ generate reports for management and customers
	6.4 Manage appropriate service improvement programmes (SIP) to overcome the difficulties and restore service quality	Be able to instigate a SIP to identify and implement whatever actions are necessary to overcome the difficulties and restore service quality

	6.5 Manage the day-to-day operations of service delivery in a professional manner	Be able to ▪ manage the day-to-day operations of service delivery in accordance with the organisation’s guidelines as well as any (local and international) laws and regulatory requirements, if applicable ▪ manage the day-to-day operations in an efficient and effective manner ▪ continuously and proactively improve on the day-to-day operations of service delivery
7. Assessment Criteria	The integrated outcome requirements of this UoCs are the abilities to: (i) ensure day-to-day operations of service delivery in accordance with the SLA; (ii) liaise with other support functions; and (iii) communicate with customers and support parties to ensure improvement requests or initiatives are taken care of.	
Remark		

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

1. Title	Conduct source selection and/or contract development
2. Code	ITSWPM523A
3. Range	Conduct source selection and further contract development in project outsourcing [Project Management – Project Procurement and Contract Management]
4. Level	5
5. Credit	5
6. Competency	Performance Requirement 6.1 Have knowledge of various evaluation methods — Be able to apply an appropriate evaluation system to the received proposals such as weighting system, screening system and independent estimates. 6.2 Identify contract concerns — Be able to rely upon methods to identify: ▪ project warranties ▪ liabilities ▪ indemnity ▪ insurance clause-related activities 6.3 Rank order to all proposals professionally — Be able to make ranking to each proposal according to the criteria as listed in the procurement management plan 6.4 Make contract negotiation with the bidder according the rank sequence — Be able to clarify any unclear points in the received proposal from the bidders and negotiate with them on the terms and conditions according to the local law 6.5 Reach mutually agreement with the bidder — Be able to make agreement on the structure and requirements of the contract prior to the signing of the contract (see remark)
7. Assessment Criteria	The integrated outcome requirements of this UoCs are the abilities to: (i) make a fair selection for a successfully bidder; and (ii) get consensus and understandings on those important terms with the successful bidder for drafting the contract.
Remark	Subjects covered generally include, but are limit to, responsibilities and authorities, applicable terms and law, technical and business management approaches, contract financing and price.

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

1. Title	Prepare a budget based on the IT plan
2. Code	ITSWSM504A
3. Range	Prepare a budget based on the IT plan for budget planning of the organization overall [Strategic Management – IT Planning and Budgeting]
4. Level	5
5. Credit	6
6. Competency	Performance Requirement 6.1 Have good knowledge of IT budget planning Be able to ▪ understand the importance of documenting an IT budget plan ▪ understand the structure of an IT budget plan 6.2 Identify the elements and information for preparing for an IT budget Be able to ▪ identify the existing available resources of the company ▪ identify the resources requirements of the IT business plan ▪ compute the cost of extra resources to acquire for budgeting ▪ conduct amortization of the current resources and factor the cost into the budget 6.3 Formulate an IT budget plan Be able to formulate plans for ▪ analyse the resource requirement above according to the IT plans ▪ develop budgetary estimates according to historical figures and lessons learnt in previous years, if available ▪ present a coherent budget plan according to industry standards
7. Assessment Criteria	The integrated outcome requirements of this UoCs is the ability to prepare a coherent budget plan according to IT business models and IT plans of the organization.
Remark	

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

1. Title	Formulate IT strategies and policies	
2. Code	ITSWSM603A	
3. Range	Formulate IT strategies and policies for an organization to support its approved business strategies and policies and to cover areas including resource optimization, business alignment, and information security [Strategic Management – Strategy Formulation]	
4. Level	6	
5. Credit	4	
6. Competency		Performance Requirement
	6.1 Understand the business strategies and policies of an organization	Be able to know the business strategies and policies of an organization with respect to business-IT alignment and enablement
	6.2 Understand international standards and regulatory requirements	Be able to understand international standards and regulatory requirements
	6.3 Understand related issues in information security and related laws of intellectual property	Be able to know related issues in information security (e.g. data security, authentication, integrity and privacy) and related laws including copyrights and IP rights etc
	6.4 Formulate IT strategies and policies of an organization	Be able to formulate IT strategies and policies of an organization to support its approved business strategies and policies including resources optimization, business alignment, and information security in compliance with necessary international standards and regulatory requirements
7. Assessment Criteria	The integrated outcome requirements of this UoCs is the ability to formulate IT strategies and policies for an organization to support its approved business strategies and policies, with profound considerations of resources optimization, business alignment, information security and regulatory compliance.	
Remark	Pre-requisite: ITSWSM602A	