Information and Communications Technology Industry

Operation and Support

Specification of Competency Standards

Second Edition

June 2025

Contents

Chapter 1

Review on Development of ICT Industry

Introduction

   The Education Bureau (EDB) of the Hong Kong Special Administrative Region (HKSAR) Government assisted the Information and Communications Technology (ICT) industry to setup its Industry Training Advisory Committee (ITAC) with a view to promoting the Qualifications Framework (QF) to the industry. In 2019, the ITAC kicked start the work of production of progression pathways and revision of Specification of Competency Standards (SCS) for the industry. In consideration of the present conditions and future development of ICT as well as the new skills and knowledge required, the above SCS formulated would not only set out the competency standards at various levels required by the future development of the industry, but also act as a set of unified benchmarks for human resources management. This could provide a comprehensive training framework for the improvement of the service quality of the industry.

2. This Section presents a review of the development of ICT industry including review of the global and local ICT industry development, the development of emerging technologies, impact on competency requirements and identification of Specification of Competency Standards (SCS) for update and development.

A Recap of the Global Development Trends of ICT Industry

3. The global ICT industry is under rapid development. Both business operations and personal lives are becoming more digital, more connected and increasingly more automated. According to the CompTIA research[1], the global ICT industry business is estimated to reach US$5.2 trillion in 2020. The United States remains the largest technology market in the world representing 32% of the total business value (approximately US$1.7 trillion). The Asia region accounts for the second largest market (21% of the total business value) with technology expenses mainly on the areas of infrastructure setup and research & development (R&D) activities. The Western Europe stays at the third position of the global technology business value with a sharing of 20%.

4. The advancement of the emerging technologies has led to the transformation of job nature and induced new skill requirements. From the Table 1.1, the top demanding new technology skills include big data analysis, app/web-enabled marketing, IoT applications, machining learning and cloud computing. According to the World Economic Forum[2], at least 133 million new ICT job roles will be generated globally by 2022 as a result of the new division of labour between humans, machines and algorithms. In addition to the strong demand of technology skills, management skills including creative thinking, problem-solving and negotiating are also highly required for the ICT workforce.

---

[1] Research Report, CompTIA (November 2019)
[2] www.weforum.org

Technology	Percentage of respondents that likely to adopt
User and entity big data analytics	85%
App- and web-enabled marketing	75%
Internet of things	75%
Machine learning	73%
Cloud computing	72%
Digital trade	59%
Augmented and virtual reality	58%
Encryption	54%

Table 1.1: Technologies by proportion of companies likely to adopt them by 2022 (projected)

(source: www.weforum.org)

5.   Filling the knowledge and skill gaps for ICT workforce is a major challenge faced by business companies worldwide.   Many companies started to develop their own training programmes to upskill their employees. The topic of ICT manpower training will further be discussed in the below paragraphs.

6.   The US ICT industry has a market-oriented economy structure mainly including extensive provision of innovative technology services across different business sectors and exports of technology products and services to other countries.   In 2018, the majority of the ICT workforce in US involves in the categories of Software, IT and Business Services, and Emerging Technologies development (Table 1.2).

Key Career Categories	ICT Workforce
Software	18%
Devices plus Infrastructure	17%
IT and Business Services	30%
Telecom Services	13%
Emerging Technologies (such as IoT, AI, Blockchain etc.)	22%

Table 1.2: ICT Key Career Categories of US market 2018 *(Source: CompTIA)*

7.   A further breakdown of the key technology employment growth drivers of the US market from 2010-2018 is shown in Table 1.3.   From the Table, the category Software Developers and Application accounts for the largest actual number of employment growth (+386,900) revealing the strong talent demand in supporting the technology service development in the past few years.   For other conventional technology positions (such as System Analysts and Network Architect), the employment growth is relatively mild.   On the other hand, it is observed that the categories Cybersecurity Analyst and Technology Occupation have high percentage increase of employment growth showing the rising needs of these new technology skills.

Key Technology Employment	Actual change	Percentage change
Software Developers and Applications	+386,900	+76%
IT Support Specialists	+190,200	+43%
Technology Occupation, Others*	+138,900	+69%
Systems Analysts	+90,000	+17%
CIOs / IT Managers	+82,900	+28%
Industrial Engineers	+69,800	+34%
Mechanical Engineers	+64,800	+27%
Web Developers	+58,800	+56%
Cybersecurity Analysts	+52,500	+91%
Network Architects	+50,800	+45%
Total	**1,185,600**	**44%**

Table 1.3: Key Technology Employment Growth Drivers in US (2010-2018) *(Source: CompTIA)*

*Note: include positions such as videogame developers, business intelligence analysts, IT project management etc.

8.   In global terms, Europe has no massive software industry[3].   However, Europe does innovate in ICT through technology applications in other industries.   For example, BMW and Airbus are the major companies embracing the Internet of Things (IoT) to develop advanced transportation systems[4].   The telecom companies such as Vodafone, Telefonica, Nokia and Ericsson are the major multinationals with telecom operations spanning several continents.   London, as one of the world's financial centers, hosts vigorous FinTech industry with keen talent demand in big data analysis and other technology-based financial services.   Ireland is the second largest exporter of computer and IT services in the world that its ICT sector accounts for more than €50 billion of the nation exports per annum[4].

9.   In 2018, around 8.9 million professionals worked as ICT specialists across the 28 member states under the European Union (EU).   In 2020, the European market is projected to be lacking more than 0.67 million ICT professionals due to the rapid growth of technology-driven business ecosystem [5].   Both small-medium enterprises (SMEs) and multinational companies are competing for ICT professionals for their business development.   Among the spectrum of job vacancies, two segments are particularly in high demand including 1) ICT professionals with strong communication and project management skills; and 2) workforce with entry-level programming skills[6].

[3] Association for Computing Machinery (2019)
[4] www.enterprise-ireland.com
[5] www.eu-startups.com (2019)

10.   To build the long-term strategic digital capacities and facilitate the wide deployment of digital technologies in EU, the European Commission has proposed the "Digital Europe Programme" with €9.2 billion of funding to support the EU ICT development for 2021-2027[6].   The Programme has identified several key areas for technology investment including supercomputing, artificial intelligence and cybersecurity.   In addition, the Programme will provide funding to nurture advanced digital skill workforce through the following initiatives.

- Support the design and delivery of short-term trainings and courses for entrepreneurs, small business leaders and the workforce
- Support the design and delivery of long-term trainings and Master's courses for students, IT professionals and the workforce
- Support on-the-job trainings and traineeships for students, young entrepreneurs and graduates.

11.   Europe is a leading region in data privacy protection.   Their General Data Protection Regulation (GDPR) provides a regulatory model that aims to protect consumers and increase control over their personal data via informed consent.   For companies with business operations in Europe, the GDPR may lead to their increased compliance risks, growing costs to maintain the data storage systems and fulfill compliance requirements.

12.   Israel is not a state member of EU but it has significant ICT development and achievement in recent years.   Israel's ICT industry was initially fueled by the defense-related research and development (R&D) needs. The Israel government has invested a lot to nurture the technology talents that it attracted many multinational companies, including Intel, IBM, Google, Cisco, Apple etc., to invest and setup research centres in Israel to take the advantage of the local talent.   Nowadays, Israel has become the global leading ICT development hub in software, data communications, hardware design and cybersecurity.   It has attracted 19% of global investment in cybersecurity, ranks number one globally in R&D expenditures per GDP, and attracts the highest rate of venture capital funding per capita in the world[7].

Development of ICT Industry in Mainland China

13.   The ICT industry is a major driving force of the Mainland China economy.   It is estimated that the Mainland China ICT market reaches $8.1 trillion in 2021 representing 55% of the national GDP [8].   The competitiveness of the Mainland China ICT companies keeps growing as the quality of domestic hardware, software, and services has continued to improve.   In 2017, the Mainland China's ICT imports totaled $528 billion while exports totaled $781 billion[10].

---

[6] www.ec.europa.eu/digital-single-market/
[7] Start-up Nation Central (SNC) and PwC Israel (2018)
[8] www.export.gov (2019)

14.   Certain technology sectors (e.g. smart phone devices) are predicted to reach saturation that could not further boost national economy growth.   It is believed that integrating ICT technologies into and transforming traditional industries will be the fuel of the future national economy growth.   As announced in the China's Made in China 2025 initiative, the industrial big data and industrial internet are the two major areas to support the new development of Mainland China's technology market[10].   Alibaba has also listed several potential technology areas for economy growth including real-time urban simulation, development and applications of AI, 5G networks for new applications, smart vehicles and commercial applications of Blockchain.   In addition, the Mainland China business companies are willing to apply and develop immersive technology (AR/VR) products for entertainment and business services markets.

15.   On the other hand, technology talent supply is a critical challenge facing by the Mainland China ICT industry.   The challenge is analyzed as below.

Gap between the talent supply and demand
According to statistics from China's National Bureau of Statistics and Ministry of Education[9], the ICT industry showed demand for a total of 7.6 million educated talents in 2017, while the number of ICT graduates per year has not yet exceeded 1 million.   There is a huge gap between the supply of talent and the demand for it, and the rapid development of the ICT industry will further widen this gap.   The overall talent deficit is projected to rise to 12.4 million by 2020[10].

Mismatch between talent quality and industry demand
As the ICT industry develops, the trend of supply chain segmentation continues to reshape the structural demand for talent.   Instead of professionals who specialize in a single area, ICT talent with diverse skill sets are expected by business companies.   Companies may look for talents who have a comprehensive knowledge of multiple areas such as technology, product, marketing, business, and communication.

16.   To fill the gap of talent supply, some Mainland China giant technology companies (such as Alibaba and Huawei) have established their own ICT training and certification programmes with training contents focusing on their own product specifications and company standards.   Beside to offering the training programmes on their own, these giant companies also seek collaboration with educational institutions to expand the supply of technology talent.

17.   The Mainland China's technology policy presents another challenge on the ICT industry development. In addition to commercial concern, the Mainland China authority would also consider national security in setting up the ICT policy.   For example:

---

[9] https://support.huawei.com/learning/news/

<u>Cybersecurity Law</u>

On June 1, 2017, Mainland China established the first Cybersecurity law as a framework to regulate China's networks on national security grounds and for the supervision of the ICT sector more generally. The law details the security obligations of internet products and service providers, institutes rules for the transmission of data, and enhances the rules on personal data protection. Lack of clarity about how the law will be enforced remains a top concern for many ICT companies in Mainland China.

18.   In view of the extensive cross-border business operations and the frequent travel between Mainland China and Hong Kong, there is a need for the Hong Kong ICT practitioners to understand the details and the compliance requirements of the relevant Mainland China's technology regulations in order to ensure smooth business operations in Mainland China.

<u>The Greater Bay Area (GBA)</u>

19.   In 2018, the Chinese Government committed to developing an international innovation and technology hub in the Guangdong-Hong Kong-Macao Greater Bay Area (GBA) that serves as a leading force for national innovation development. To support the GBA development, the China Government has announced the following technology initiatives:

- strengthen the coordination of policies in areas such as intellectual property protection, market regulation, financial technologies, talent cultivation and the commercial application of technological achievements
- establish several major technological infrastructure facilities, cross-study platforms, as well as emerging innovative research in the GBA
- remove barriers that hinder the free flow of talent, technologies, capital, equipment, information and other innovative elements in the GBA

20.   According to some study reports[10&11], the GBA has a high proportion of high level talent in the areas of manufacturing, consumer goods and ICT with over 25 percent having overseas learning experience and more than 30 percent holding a master's degree and above. Among the ICT relevant specialties, the majority of the talent possesses computer science qualification.

21.   The reports pointed out that the demand for quality technology workforce in the GBA is particularly acute in four fast-growing industries including research and development within innovative technologies, financial services, trade and logistics, and the medical industry. R&D in technology lacks of professionals in areas of data scientists, cloud architects, user interface designers, solution engineers and artificial intelligence. There is a need to upgrade the gap of the current technology workforce in the GBA.

---

[10] GBA talent study report by the Tsinghua University's School of Economics and Management and LinkedIn in 2019
[11] Decoding the Outline Development Plan for Guangdong-Hong Kong-Macao Greater Bay Area 2019

22.   The reports examined that among the GBA eleven cities, Shenzhen, Guangzhou and Hong Kong are rated as the top cities where digital talent is concentrated.   It is further analyzed that Guangzhou has the most balanced talent distribution among industries; Shenzhen highlights the talent in ICT relevant industries while Hong Kong mainly has talents in the financial and education industries.

23.   According to the reports, the number of talent exchange between Hong Kong and other GBA cities lags far behind that of Shenzhen and Guangzhou.   There is room for Hong Kong to further strengthen talent exchange with other GBA cities especially the necessity for favorable policies to incentivize the youth of Hong Kong.

24.   In summary, the development of emerging technologies is changing the global business ecosystem. Different nations have been setting up policies to support and upgrade the ICT skill workforce training.   The demand for ICT workforce with new skills/knowledge is keen especially in the areas of big data analysis, AI, cybersecurity, IoT applications and cloud computing etc.   Business companies has also positioned ICT as an integral part of their strategy planning process that the ICT workforce is also expected to enhance their competence in business management.   In addition to university academic path, industry professional training/certification could be considered as an alternative pathway to fill up the technology gap of ICT workforce. If university programmes and/or industry certifications are developed with reference to industry competence standard, it would facilitate the recognition of the outcomes of training by the industry.

Development of ICT Industry in Hong Kong

25.   In 2017, the ICT industry generated US$13.6 billion of value added, contributing to round 4% of the Hong Kong GDP.[12]   The ICT infrastructure of Hong Kong plays an important role to maintain its leading business position in the Asia-Pacific region especially in the age of e-business and digital social media.   According to the Global Innovation Index 2019, Hong Kong ranked fourth worldwide in technological infrastructure.   The ranking indicates the readiness of the Hong Kong's infrastructure and market to support the development of digital economy.

26.   In the following paragraphs, the Hong Kong ICT industry would be reviewed from the public policy, economic, social and technological aspects to explore the future development direction of the industry.

Public Policy Factor

27.   Focusing on technology related public policies, the two major initiatives including the Hong Kong Smart City Blueprint and the Greater Bay Area would definitely impact on the coming Hong Kong ICT industry development and the technology talent requirements.

---

[12] "2018 Economic Background and 2019 Prospects", HKSAR Government

<u>Smart City Blueprint</u>

28.　　In 2017 the HKSAR Government published the Smart City Blueprint[13] outlining the Government's vision to build Hong Kong into a world-class smart city. The Blueprint covers six areas including "Smart Mobility", "Smart Living", "Smart Environment", "Smart People", Smart Government" and "Smart Economy". Three digital infrastructures will be developed to support the Smart City Blueprint including "eID", "Pilot Multi-functional Smart Lampposts Scheme" and "Next Generation GovCloud and Big Data Analytics Platform".

29.　　According to the study by Sharing Economy Alliance[14] in 2018, Hong Kong came last in developing innovation and technology out of other Asian cities such as Taipei, Shenzhen, Seoul and Singapore. Lack of sufficient technology talent supply is considered as a major factor of holding back the Hong Kong smart city development. According to a study report[15], over 70% of the Hong Kong CIOs commented that IT security, software/application development (including Java/Python developers and UI developers etc.) and database management are the most difficult functional areas to source skilled IT workforce.

30.　　To support the ICT industry development and talent development, the HKSAR Government has announced the following policies in recent years.

2017 Government Policy Address
▪ Earmarked HK$500 million for the Innovation and Technology Bureau (ITB) to help the government in applying technology to improve the quality of public services
▪ Promoted establishment of a Common Spatial Data Infrastructure (CSDI) to enable sharing of geospatial data and support the Smart City Blueprint of Hong Kong
▪ Introduced the Technology Voucher Programme to facilitate the adoption of technology by small-and-medium enterprises (SMEs) for upgrading and improving productivity

2018 Government Policy Address
▪ Injected $20 billion into the Research Endowment Fund of the Research Grants Council and launched a $3 billion Research Matching Grant Scheme
▪ Expedited re-industrialization by establishing a $2 billion re-industrialization funding scheme to subsidize manufacturers to set up smart production lines in Hong Kong and allocating $2 billion for building manufacturing facilities required by the advanced manufacturing sector in industrial estates
▪ Promoted technology transfer by increasing the funding support to the Technology Transfer Offices of universities, the Technology Start-up Support Scheme for Universities, as well as the State Key Laboratories and Hong Kong branches of the Chinese National Engineering Research Centre

---

[13]　https://www.smartcity.gov.hk/
[14]　https://sharingcitiesalliance.com/
[15]　Robert Half Technology Salary Guide 2019

2019 Government Policy Address
- Extended the coverage of the Technology Talent Admission Scheme to companies outside the Hong Kong Science and Technology Parks Corporation and Cyberport and to cover new technology areas
- Extended the coverage of the Researcher Programme, Postdoctoral Hub and Public Sector Trial Scheme to all technology companies conducting research and development activities
- Injected $500 million into the Social Innovation and Entrepreneurship Development Fund to further promote social innovation

2018-19 Government Budget
- The Government identified four areas for technology development including biotechnology, artificial intelligence, smart city and financial technologies (Fintech).   Additional funding was allocated to promote the innovation and technology development that include:
  - HK$10 billion additional injection to the Innovation Technology Fund (ITF)
  - HK$10 billion to support the establishment of two research clusters on healthcare technologies, artificial intelligence and robotics technologies
  - HK$200 million to Cyberport to enhance support for start-ups and promote development of a digital technology ecosystem
  - HK$100 million to Cyberport to promote the development of eSports

Integration with the Greater Bay Area (GBA)

31.   Shenzhen has a strong pool of ICT talent while Hong Kong mainly has talents in the financial and education industries.   The Hong Kong Government has reviewed its role in the GBA development by changing from a connector to being a more proactive participant with the following technology related initiatives[16].

32.   The four fast-growing industries in the GBA includes research and development of innovative technology, financial services, trade and logistics, and the medical industry.   The above initiatives by the HK Government could support the technology talent demand of R&D activities, FinTech and trade and logistics.   On the other hand, Hong Kong has existing advantage of providing high standard medical service.   Future development of digitalization of the industry operation should have great potential market in Hong Kong and the GBA.

33.   The development of Hong Kong Smart City and the GBA would continuously drive substantial demand of technology talent.   It is observed that the Hong Kong's R&D investment has kept improving.   According to the WIPO (World Intellectual Property Company)[17], Hong Kong ranked 13th worldwide under the Global Innovation Index (GII)[18] in 2019 as compared to 16th in 2017.   The ranking in 2019 is also the third position in Asia that just

---

[16] Decoding the Outline Development Plan for Guangdong-Hong Kong-Macao Greater Bay Area 2019
[17] Global Innovation Index (2019)
[18] https://www.globalinnovationindex.org/Home

behind Singapore and South Korea. On the other hand, together with the Shenzhen innovation and technology sector, the Shenzhen-Hong Kong technology cluster ranked the world's second largest on the GII 2018. It is expected the continuous investment on R&D schemes could further support the R&D talent supply for the ICT industry growth.

Other Government Policies

34. In the 2017-18 Budget, the Financial Secretary highlighted eSports as a new potential sector to boost the local digital entertainment and ICT industries. The Hong Kong Government has injected a funding of HK$100 million to Cyberport to promote the development of eSports. Although Hong Kong is not a major game development hub, the development of eSports industry could induce other demand of technology talent including digital content production, social media marketing, network infrastructure setup and online broadcasting etc.

35. The Hong Kong's start-up ecosystem keeps growing in recent years with the increasing funding supports. According to the survey by InvestHK[19], in 2017, there is a record of steady growth of the number of start-ups (+16%) and the number of staff employed in these start-ups (+21%) as compared with the previous year. Major focus of the Hong Kong ICT start-ups includes software as a services (SaaS), Internet of Things (IoT), data analytics, biotech, Artificial Intelligence (AI), robotics, Virtual Reality (VR) and Augmented Reality (AR). In terms of application development, Fintech, Smart City and Smart Home, healthcare and big data applications are also popular. The growth of the local start-up ecosystem is benefited by the increasing investment on R&D activities from the Hong Kong Government, and the global and local trend of emerging technology applications in finance and e-business sectors.

Economic Factors

36. The high rent in Hong Kong has speeded up the companies' pace to develop e-business[20] in order to reduce the rental cost. It is estimated that the revenue in the Hong Kong e-business market amounts to US$4,784 million in 2019 while the revenue is expected to show an annual growth rate of 7.9%, resulting in a market volume of US$6,484 million by 2023[21]. To catch up the rapid growth of e-business market, business companies have to consider which technologies fit into their business the best. According to a study report (Table 1.5), building omni-channel business platforms and social media platform for consumer engagement are the most important concern by Hong Kong companies, followed by big data application development. The rapid development of e-business depends on the supply of technology talent including digital media production and marketing, big data applications and mobile apps development etc..

---

[19] https://www.investhk.gov.hk/en.html
[20] Definition of e-business: "all business activities conducted through electronic means, including all business activities involved in various stages of the business cycle from marketing, advertising, ordering, delivery, payment to stock replenishment." (www.legco.gov.hk)
[21] KPMG and GS1 Survey Analysis (2017)

Area		Percentage
1	Building omni-channel business platforms	31
2	Popular social media platform for consumer engagement	25
3	Adopting big data analytics	17
4	Building up mobile commerce	11
5	Adopting Internet of Things	9
6	Adopting cloud computing technologies	6
7	Others	1

Table 1.5: The most important digital innovation technology for business development

(Source: KPMG and GS1 Survey Analysis (2017))

37.　　　Online cross-border trading is another growth area for the Hong Kong business companies especially for e-business in China.　According to Agreement Ten of the Mainland and Hong Kong Closer Economic Partnership Arrangement (CEPA) Supplementary[22], service providers in Hong Kong are allowed to set up joint ventures to provide online data processing and transaction processing business (operating e-business sites) in Guangdong province.　Hong Kong business companies could make use of the support from CEPA to strengthen the development of the cross-border e-business in the Mainland.

38.　　　More companies are entering the Hong Kong's FinTech sector to offer innovation solutions to the local and global markets in areas such as payment systems and data analytics.　To support the development of Hong Kong FinTech market, the Hong Kong Monetary Authority (HKMA) has launched the upgraded version of the FinTech Career Accelerator Scheme to nurture the talent.　In addition, in the 2017-18 Budget, the Hong Kong Government has provided HK$2 billion for the technology start-ups to support the FinTech industry.　It is expected that the talent demand in relevant FinTech areas would keep growing.

39.　　　Hong Kong is developing data center business by taking its advantages including location as an international investment hub, free flow of information and proximity to the Mainland China.　The development drives the talent demand of data scientists and cyber security specialists.

40.　　　It is also observed that more Hong Kong technology and business companies are moving towards to a more Agile methodology of project-based work to replace the waterfall management approach.　Companies hiring management staff are therefore, looking for candidates who are not only technically capable but also have the software skills (such as collaboration and adaptability etc.) to work in an Agile workplace.

---

[22] "Overview of Internet in Hong Kong", HKTDC Research

41.　　On the other hand, the Mainland China recorded a slowdown of economy growth with the 2018 GDP at 6.5% only, which is the lowest in the past 28 years.　　However, the giant technology company Alibaba reported that their ebusiness sales volume was still under double-digit growth despite the overall slowdown of the nation economy.　　Alibaba commented that their business growth heavily depends on the rapid and diversified development of ebusiness marketing channels.

Social Factors

42.　　Social factors, including population statistical data such as the age of population and its distribution, their education, living attitude and consumption pattern, etc., will affect the preference of consumers, thus influencing their demands on different products and services.

43.　　Hong Kong's communications and Internet infrastructure is advantageous to the development of online shopping, especially for the younger generation.　　According to a survey[23], Hong Kong ranked tenth in the Asia Pacific region on the popularity of online shopping (with China ranked the first and India ranked the second).　　By considering the factors affecting online shopping behavior, secure payment facility remains to be a top factor, along with the reputation of the website or merchant and the items' prices or monetary value.　　As online shopping continues to develop as one of the most significant consumption activities in Hong Kong, it would further drive the demand of technology talent in areas of digital media production, digital marketing, cybersecurity and mobile apps development etc.

Technology Factors

44.　　The comprehensive and advanced ICT infrastructure in Hong Kong includes the 100% coverage of mobile network, the fastest Internet connection speed in the world, numerous free public Wi-Fi points and high mobile device penetration rate.

HK ICT Infrastructure	Figures
Mobile Services	
▪ Mobile network operators	4
▪ Mobile subscriber penetration rate	259.9%
▪ Mobile broadband customers (2.5G/3G/4G)	18,573,243
Internet Services	
▪ Registered customer accounts with broadband access	2,699,029
▪ Household broadband penetration rate	93.2%

Table 1.6: Key statistics of ICT infrastructure in Hong Kong

(Source: Office of the Communications Authority)

---

[23] "Hongkongers Continue to Embrace Online Shopping", Mastercard Survey (2018)

45.　　　The ICT infrastructure could well support local and overseas business companies to carry out frequent e-business activities and foster the development of technology-based business applications.　With the growing demand on obtaining faster and reliable consumer service, business companies are driven to further develop business and technology applications.　In addition, Hong Kong's advancement of data centre and cloud computing service also supports business companies to develop innovation and technology initiatives to meet the local and global business opportunities brought by emerging technologies.

Impact on Competency Requirements and Manpower Development in Hong Kong

46.　　　The increasing adoption of internet stimulated the growth in all facets of economic interactions that achieving the global transferability of skill and knowledge.　The ICT industry itself also breaks the geographical constraint especially through the flourishing global outsourcing services.　An advantage of the Hong Kong ICT professionals is their language competency of Chinese and English communication that enable them to work with clients from Mainland China and other countries.　The language competency is important in matters of collection and preparation of the system specifications, communication with clients and preparation of the user manual etc. In particular, the China Government's initiative to develop the Greater Bay Area (GBA) into an international innovation and technology hub would continuously drive substantial demand of technology talent.

47.　　　ICT is a vast sector that is continuously splintering off into subsectors.　There is an array of career paths for professional development.　As the impact of digitalization is growing exponentially, the global technology manpower demand is keen.　ICT professionals could develop themselves into different technology specialists to catch the new technology career opportunities.　On the other hand, ICT is a team-based industry requiring professionals with transversal skills including communication, problem solving, collaboration, project management and team skills.　The ICT professionals could also further develop their career into different managerial positions.

48.　　　Major emerging technologies, including Blockchain (distributed ledger technology), Artificial Intelligence (AI), Virtual Reality (VR), Internet of Things (IoT), 5G network and Cloud computing etc., are rapidly redefining global business and society development.　The new business ecosystem however, has brought several challenges to the business companies today including the demand of production efficiency, expansion into new markets and the competition on new products for a global consumer base.　Business companies have to consider which technologies fit into their business the best.　They have to place more priority on how technologies could support potential market penetration across different channels, how to apply the technologies to enhance customer services and how technologies could innovate their business.　Large number of ICT professionals now are therefore, employed by companies from different industry sectors.　For instance, the IDC Research (IDC FutureScape: WorldWide IT Industry 2019) indicated that 46% of the US ICT workforce is employed by technology companies while 56% of the ICT workforce is employed by companies from different industry sectors.

49.   The increasing adoption of ICT in government and public utility organizations has brought advancement in public service standard in terms of improving efficiency and transparency.   To deliver more robust and user-friendly digital services to citizens, many cities have been increasing the investment on technology hardware and manpower development.   A stable source of ICT professionals is crucial to deploy and maintain these digital services as any failure of the systems, such as the electricity and telecommunication systems, would bring adverse impact to the society operation.   Therefore, there is a need to have a well-established framework to develop and monitor the competency requirements for the ICT professionals, and to recognize their standard of competency, particularly in the new technology areas.

50.   The advancement of the emerging technologies has led to the transformation of job nature and induced new skill requirements.   From the Table 1.1, the top demanding new technology skills include big data analysis, app/web-enabled marketing, IoT applications, machining learning and cloud computing.   According to the World Economic Forum[24], at least 133 million new ICT job roles will be generated globally by 2022 as a result of the new division of labour between humans, machines and algorithms.   In addition to the strong demand of technology skills, management skills including creative thinking, problem-solving and negotiating are also highly required for the ICT workforce.

Technology	Percentage of respondents that likely to adopt
User and entity big data analytics	85%
App- and web-enabled marketing	75%
Internet of things	75%
Machine learning	73%
Cloud computing	72%
Digital trade	59%
Augmented and virtual reality	58%
Encryption	54%

Table 1.1: Technologies by proportion of companies likely to adopt them by 2022 (projected)
(source: www.weforum.org)

Identification of Competency Standards for Updating and the Vocational Qualifications Pathways (VQP)

51.   Having reviewed the development of ICT industry and the impact of development of emerging technologies, this section provides a suggested list of emerging areas and management skills for updating the competency standards in order to support the Hong Kong ICT industry development, and for the technology workforce catching up with the competence requirements in view of technology development.   To make sure the competency requirements are relevant and applicable to that of principal job posts in the industry, the VQP under respective emerging area has been drawn up with reference to the Manpower Survey Reports and in consultation with relevant stakeholders to serve as a basis for working out the competency requirements.   The emerging areas

---

[24] www.weforum.org

and management skills identified are listed below:

1	Emerging Area	AI/Machine Learning
	Proposed Functional Area(s)	Design, Development and Maintenance / Software Products & Software Services Application Support / Operation and Support
	Details of competency requirements	Architecture design of the software/system, requirement identification of software release, risk assessment, testing, online payment, payment security

2	Emerging Area	Cloud Computing
	Proposed Functional Area(s)	Architecture / Software Products & Software Services Network Support / Operation and Support
	Details of competency requirements	Cloud adoption – infrastructure concern, business workflow reconfiguration, risk management and resources optimization for cloud computing

3	Emerging Area	Information Security
	Proposed Functional Area(s)	Information Security / Software Products & Software Services Security Support / Operation and Support
	Details of competency requirements	Cybersecurity policy setup, evaluation and management of cybersecurity threats, development and implementation of security measures, plan for disaster recovery, stakeholder management in relation to cybersecurity issues

4	Emerging Area	Data Science
	Proposed Functional Area(s)	Design, Development and Maintenance / Software Products & Software Services Application Support / Operation and Support
	Details of competency requirements	Database administration, predictive analytics, data visualization, data management/policy

5	Emerging Area	eSports Technology
	Proposed Functional Area(s)	DMT architecture / Digital Media Technology
	Details of competency requirements	Network infrastructure setup, online broadcasting, cost optimization, troubleshooting,

6	**Emerging Area**	**Internet of Things (IoT)**
	Proposed Functional Area(s)	Architecture / Software Products & Software Services Systems & Hardware Support / Operation and Support
	Details of competency requirements	Business operation model with IoT, hardware/software requirements

7	**Management Skills**	
	Proposed Functional Area(s)	Strategic Management / Software Products & Software Services Project Management / Software Products & Software Services
	Details of competency requirements	Innovation management, the role of ICT in business strategy setup, regulatory compliance (including Mainland China and Europe Union ICT policies)

-END-

Chapter 2

Units of Competency

Title	Perform next level escalation
Code	107860L1
Description	This unit of competency applies to IT support personnel who are responsible for providing technical support to users. All supporting personnel will need to understand and follow the organisation's escalation procedure so that he/she will have a guidance as when, how and whom to escalate to when in need of assistance. This UoC is concerned with technical issues escalation. Note: every organisation have different escalation procedures that corresponds to their business needs; some escalation procedures may even require support personnel to perform drills to ensure that the procedure is effective
Level	1
Credit	1

Competency	Performance Requirements
	1. Knowledge to perform next level escalation
	
	• Possess good communication, listening, literacy and written skills
	• Possess basic knowledge of the organisation support service procedures
	• Understand the importance of following procedures and team work when providing user support
	2. Perform next level escalation
	
	• Understand Service Level Agreement (SLA) set by the organisation or department
	• Comprehend the organisation escalation procedure. Example of contents in an escalating procedure:
	    o Contacts details of different level of escalation
	        ▪ Level 1 support contact person and contact details
	        ▪ Level 2 support contact person and contact details
	        ▪ Level 3 support
	        ▪ Supervisor
	    o Stages and situations to trigger escalation, such as when and what will need to escalate to level 1 and when and what to level 2, etc.
	    o Work with documents for escalation, such as escalation initiation form, etc.
	• When escalating during a support session, follow the organisation escalation procedure and complete necessary documents as when required
	• Participate in escalation drills if when required
	3. Exhibit professionalism
	
	• Possess customer service oriented attitude and escalate just at the right time
	• Committed to improve quality services to users and customers

Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Comprehend the organisation's escalation procedures and understand when, how and whom to escalate from the guidelines of the procedure • Effectively perform escalation to ensure SLA of the organisation or department are achieved • Complete all necessary escalation documents in accordance with the organisation standards
Remark	

Title	Understand the System Development Life Cycle for technical support
Code	107861L1
Description	This unit of competency applies to all IT practitioners providing technical support at work place. IT practitioners encounter many different life cycles in their industry and one of the most important life cycle is System Development Life Cycle (SDLC). Operation support and service personnel need to appreciate the concept of SDLC and how it affects them
Level	1
Credit	1

Competency	Performance Requirements
	1. Knowledge for understanding the System Development Life Cycle for technical support
	
	• Possess good literacy skills that can read various product technical manuals, work instructions, work procedures, organisational guidelines and procedures, etc.
	• Possess logical thinking and diagnostic skills
	• Possess basic knowledge of Occupational Safety procedures
	2. Understand the System Development Life Cycle for technical support
	
	• Understand the stages of the SDLC and variants/adaptations of SDLC, such as:
	   ○ Equipment Life Cycle
	   ○ Production Life Cycle
	   ○ ICT Life Cycle
	   ○ PC life Cycle
	• Understand why SDLC is important, including but not limited to the following:
	   ○ Project management
	   ○ Cost management
	   ○ Time management
	   ○ Human resources management
	• Understand mapping of SDLC with respect to Operation Support and Service personnel daily activities, including but not limited to the following:
	   ○ Equipment/service request
	   ○ Equipment/service purchase
	   ○ Installation
	   ○ Configuration
	   ○ Support
	   ○ Maintenance,
	   ○ Equipment retirement
	3. Exhibit professionalism
	
	• Committed to resolve problems
	• Follow organisation safety guidelines and procedures when troubleshooting and/or performing rectification of equipment

Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Understand the basic concept and objectives of the SDLC and aware of different variants or adapted life cycles and where it affects them in their daily work activities • Map work activities of support and service personnel with the different stages of SDLC or variants
Remark	

Title	Understand the principle of troubleshooting
Code	107862L1
Description	This unit of competency applies to all IT personnel who are involved in production work such as: technical support, software development, system installation, etc. There are many kinds of troubleshooting, including: configuration troubleshooting, program troubleshoot (debugging), system troubleshooting, network troubleshooting, etc. The specific troubleshooting that required specialised technical skills will be covered elsewhere. This UoC is concerned with general principles of troubleshooting which illustrates the common competencies for troubleshooting
Level	1
Credit	3

Competency	Performance Requirements
	1. Knowledge for understanding the principle of troubleshooting
	
	• Possess good literacy skills that can read various product technical manuals, work instructions, work procedures, organisational guidelines and procedure, etc.
	• Possess basic communications for liaising with users or vendors
	• Possess logical thinking and diagnostic skills
	• Possess basic knowledge of hardware, OS and system scripting
	• Possess basic knowledge of Occupational Safety procedures
	2. Understand the principle of troubleshooting
	
	• Understand the problem from:
	    o User
	    o Program result
	    o Problem log/report
	    o Symptoms
	• Understand the importance to verify the problem actually does exist using combination of techniques including but not limited to the following:
	    o Reproduce the problem
	    o Systematic questioning user
	    o Apply tools to detect the problem
	    o Study reports and event logs
	    o Analyse error messages
	• Understand the use of different techniques to perform fault finding and produce a list of probable causes, including but not limited to the following:
	    o Visual checks
	    o Use fault finding tools to collect and analyse data
	    o Analyse the logic of software against program design
	    o Program testing
	• Understand the next step is planning to resolve problems including making provision for rollback when applied solution fails to correct the problem
	3. Exhibit professionalism
	
	• Committed to resolve problems
	• Follow organisation safety guidelines and procedures when troubleshooting and/or performing rectification of equipment

Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Understand the principle of troubleshooting and can systematically follow troubleshooting steps to verify and locate the problems

	• Understand that solutions can only be offered when one can correctly diagnose the probable cause of the problem
Remark	

Title	Understand the principle of data security
Code	107863L1
Description	This unit of competency applies to all IT practitioners being responsible, handling or work with data. They need to understand that data is one of the most important assets of the organisation it must be protected. To be in a position to protect the organisation assets, they need to be aware of the data vulnerabilities. In addition, they need to understand personal ethics and apply industry best practices are important to the security of the organisation's data
Level	1
Credit	1

Competency	Performance Requirements
	1. Knowledge for understanding the principle of data security
	
	• Possess good literacy skills that can read various product technical manuals, work instructions, work procedures, organisational guidelines and procedure, etc.
	• Possess basic communications for liaising with users or vendors
	2. Understand the principle of data security
	
	• Understand data is the asset of organisation and the importance of data
	• Understand vulnerability and risks of data, such as:
	    o Theft
	    o Loss
	    o Negligence
	    o Insecure practices
	• Understand security principles, including:
	    o Confidentiality
	    o Integrity
	    o Authentication
	    o Non-repudiation
	    o Availability
	    o Accessibility
	• Understand different data security protections and techniques
	• Understand the organisation's data security guidelines and procedures
	• Understand international data and information security standards. For example: ISO 27001
	• Understand the importance of being ethical and apply industry best practices for data security in work place
	3. Exhibit professionalism
	
	• Committed to protect the assets of the organisation by following and complying with organisation and regulatory security standards
	• Be an advocate of data security and protection

Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Understand different vulnerabilities of the organisation's data • Understand the importance of possessing good security practices and ethics to ensure the organisation data is protected
Remark	

Title	Understand the principle of data protection
Code	107864L1
Description	This unit of competency applies to all IT practitioners being responsible for, handling or working with personal data. In the age of big data and Internet of thing (IoT) personal information are everywhere and potentially be misused; All practitioners should understand and comply with the data protection principles, as do the organisation they work for, when collecting, holding, processing or using personal data in Hong Kong.
Level	1
Credit	1

Competency	Performance Requirements
	1. Knowledge for understanding the principle of data protection:
	
	• Possess good literacy skills that can read various product technical manuals, work instructions, work procedures, organisational guidelines and procedure, etc.
	• Possess basic knowledge of data security
	• Possess basic knowledge of Occupational Safety procedures
	2. Understand the principle of data protection
	
	• Understand why there is a need for data protection, such as privacy requirements applicable to data of their customers, employees and suppliers
	• Understand Hong Kong Personal Data (Privacy) Ordinance. In particular when collecting, holding, processing and using personal data, businesses should comply with the data protection principles set out in the Ordinance relating to:
	    o the purpose and manner of collection of personal data
	    o the accuracy and retention of personal data
	    o the use of personal data
	    o the security of personal data
	    o information that should be made generally available
	    o access to personal data
	• Understand and comply with the organisation's data protection policies
	• Understand security protection requirements when handling personal data and apply suitable data security techniques with industry best practices for optimal protection that comply with the organisation and regulatory requirements
	3. Exhibit professionalism
	
	• Committed to take all practicable steps to ensure that personal data is protected from unauthorised or accidental access, processing, erasure, loss or use
	• Participate to improve the organisation's data protection procedures

Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Understand why data protection is important and the need for data protection policies in an organisation • Understand the principles of data protection
Remark	

Title	Understand professional ethics and conducts
Code	107865L1
Description	This unit of competency applies to IT support personnel. IT professionals of all levels must appreciate the importance of professional ethics and to comply with professional code of conducts at workplace.
Level	1
Credit	3

Competency	Performance Requirements
	1. Knowledge for understanding professional ethics and conducts:
	
	• Possess good literacy skill that can understand technical and non-technical documents
	• Possess good knowledge of the organisation's culture and ethics
	• Possess good knowledge of the organisation's code of conducts
	• Understand the importance of compliance of professional ethics and code of conducts
	2. Understand professional ethics and conducts
	
	• Observe code of conducts related to professional interests, included but not limited to the following:
	   o Follow the 10 commandments of computer ethics, such as:
	      ▪ Not use computer to steal
	      ▪ Not use computer to harm people
	      ▪ Not interfere with other people's computer work
	      ▪ Etc.
	   o Perform duties with integrity, trustworthy and honesty, due care and diligence. Avoid any situations which could lead to conflict of interest
	   o Have knowledge of professional standards, ethics and relevant legislations related to professional activities
	   o Honour and not knowingly infringe property and copy rights
	   o Respect confidentiality and not disclose or use for personal gains
	   o Report or seek advice from supervisor when observed a breached of organisation's code of conducts or irregularities
	• Observe code of conducts related to public interests, included but not limited to the following:
	   o Conduct professional activities:
	      ▪ with due regards for public health, privacy, security and wellbeing
	      ▪ without discrimination on sex, sexual orientation, marital status, nationality, colour, race, ethnic origin, religion, age or disability
	      ▪ With due regards to personal data privacy,
	      ▪ Carryout adequate protection of personal data in terms of collection, retention, security and use
	• Observe code of conducts related to legal interests, included but not limited to the following
	   o Be familiar and abide laws of relevant professions, including but not limited to the following:
	      ▪ Personal Data (Privacy) Ordinance
	      ▪ The Unsolicited Electronic Message Ordinance
	      ▪ Prevention of Bribery Ordinance
	      ▪ Computer Crime Ordinance
	      ▪ Intellectual Property Related Legislation (Trademarks laws, Patents Laws, Registered Design Laws, Copyright Related Legislation)

	3. Exhibit professionalism • Adhere to the organisation's professional conducts and followed all work procedures and standards

Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to:
	
	    • Observe and follow the organisation's code of conductions when performing professional duties
	    • Be knowledgeable of public interest related codes of conducts and ethics
	    • Be knowledgeable of legal interest codes of practice

Remark	

Title	Keep user/client informed of status of work
Code	107866L2
Description	This unit of competency applies to IT personnel who provides work status to users or clients where users can be different categories of internal and/or external. The type of work can be: support, installation, maintenance work or production work. The format and the timing of work status depends on the type of work and length of work which the practitioners need to judge.
Level	2
Credit	1

Competency	Performance Requirements
	1. Knowledge for keeping user/client informed of status of work
	
	• Possess good communication and interpersonal skills
	• Possess good written skills
	• Possess basic knowledge of the organisation's guideline for customer support
	• Understand and appreciate the importance of providing work status
	2. Keep user/client informed of status of work
	
	• Comprehend the organisation's guidelines and procedures for customer service and understand why the need to keep user/client informed of work status, included but not limited to the following reasons:
	   o Trigger start of work or signify end of work
	   o Allow user/client to plan:
	      ▪ their schedule
	      ▪ contingencies
	   o Provide transparency of work
	   o Personal professionalism
	   o Organisation's image
	• Select the appropriate format and length of work status, including but not limited to the following:
	   o Formal project report
	   o Verbal (face to face, phone call, recorded message, etc.)
	   o Simple sign (nod of the head, thumbs up, etc.)
	   o Short written note (on standard form, email, plain paper, etc.)
	• Determine appropriate time to communicate the work status
	   o Start of work
	   o End of work
	   o Different stages/phases of work
	• Determine the level of detail for the communication of work
	• While communicating the work status, ensure the user/client:
	   o Receive the reported status
	   o Understand the reported status
	3. Exhibit professionalism
	
	• Always protect the interest and image of the organisation
	• Always ensure user/client aware of the status of the work

Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Understand the importance of keeping user/client informed of work status • Provide work status to user/client in the correct format, correct level and at appropriate time

Remark	

Title	Provide support to users
Code	107867L2
Description	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: o 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 o Patience: users have wide range abilities. Hence, some users will require extra efforts to support o 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 o Stay confident: to provide the impression that the problem is not serious and transfer the confidence to the user o Time management: knowing how long to spend on the issue or troubleshooting before escalate for assistance o 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: o Complete all the required documents in accordance with the organisation's procedures, such as problem reports, etc. o Liaising with vendors for product information, parts, etc. o Liaising with service providers on purchased service o 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

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	

Title	Work with service providers/vendors/developers
Code	107868L2
Description	This unit of competency applies to junior Information Technology (IT) personnel who have a need to work with service providers, vendors or developers on different matters, including acquisition of product information, purchasing of equipment, and follow up issues. It is essential to maintain good relationship with suppliers, vendors or developers. However, one must be cautious, exhibit professionalism, but not violate organisation guidelines. Unless for small purchase, IT personnel of this level who is involved in the procurement process is expected mainly playing the role of assisting in the purchasing process rather than deciding or authorising the purchase.
Level	2
Credit	3
Competency	Performance Requirements 1. Knowledge for working with services/vendors/developers: - Possess good literacy, communication, interpersonal and negotiation skills - Possess detail knowledge of the organisational contract negotiation policies and guidelines - Possess good experience with organisation's procurement procedures and guidelines - Understand different methodologies for measuring and monitoring supplier performance - Possess good knowledge of IT product and trends - Possess good knowledge of the government guidelines on Prevention of Bribery Ordinance and Clean Business Practices 2. Work with service providers/vendors/developers - Seek product information from suitable suppliers, vendors or developers - Communicate in a friendly manner - Convey precisely what product information is needed as well as providing accurate and correct receiving communication details - Collect and/or document product information from suppliers, vendors or developers - Assisting procurement process - Follow the organisation's guideline to formulate Request for Quotation (RFQ) including: - Identify the required number of quotations needed (may depend on the cost of product) - Determine the method of seeking quotations (tendering, verbal, written, etc.) - Create the RFQ documents - Identify and liaise with suitable suppliers, vendors or developers that are willing to receive RFQ. - Send the RFQ to suppliers, vendors or developers and follow up to ensure RFQ has been received - Process the returned quotations fairly and equally, including: - Formulate a comparison document containing the RFQ specification items in order priority - Systematically map the RFQ items against the returned quotations - Identify and highlight any items needed special attention - Package all sourced information with RFQ comparison and forward to appropriate stakeholders for decision making

	• Follow up on issues and discrepancies
	    ○ Identify and investigate causes of issues and discrepancies with suppliers, vendors or developers
	    ○ Negotiate and resolve the issue, positively. Amendment on previous agreement may be required.
	    ○ Document agreement and amendment
	    ○ Communicate approved amendments to suppliers, vendors or developers and relevant stakeholders
	3. Exhibit professionalism
	
	• Exhibit professional ethics when handling such as:
	    ○ All suppliers are treated equally
	    ○ All tenders are followed-up fairly
	    ○ etc.
	• When procuring products always follow the organisation's and the ICAC guideline
	• Always look after the interest of the organisation

Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Use tactful skills when dealing with supplier, vendors or developers during information seeking • Follow the organisation guidelines when dealing with suppliers, vendors or developers • Achieve the objectives and maintain good relationship with suppliers, vendors or developers
Remark	IT personnel involved with procurement cycle should refer the following UoC and applies the good practices: 107871L3 – Implement "clean" business practices, good control and integrity management

Title	Comply with anti-bribery law and adopt a high standard of integrity in the operation and procurement of ICT products and services
Code	107869L2
Description	This unit of competency (UoC) is applicable to staff involved in the operation and procurement of ICT products and services in an organisation. It involves a basic understanding of the importance of compliance with the law, key provisions of the anti-bribery law in Hong Kong as well as ethical and integrity requirements; an awareness of the related challenges that may arise in the work environment in the industry, and knowledge of how to deal with them; and development of a high standard of integrity, and an ethical as well as law-compliant culture.
Level	2
Credit	1
Competency	Performance Requirements 1. Knowledge of the anti-bribery law in Hong Kong, ethical and integrity requirements, and the related challenges: • Understand the importance of compliance with the law and business ethics to the proper functioning and well-being of individuals, businesses, and society • Understand the key provisions of the Prevention of Bribery Ordinance • Understand the values, requirements and expectations of business ethics, including fairness, justice, impartiality, integrity, fiduciary duty, confidentiality, etc. • Understand the importance of complying with the organisation's code of conduct and house rules 2. Comply with anti-bribery law and adopt a high standard of integrity in the operation and procurement of ICT products and services • Develop a law-compliant and ethical culture, and a high standard of personal integrity • Ensure that one's performance of duty and personal behaviour complies with the Prevention of Bribery Ordinance and related laws • Ensure that one's performance of duty and personal behaviour complies with business ethics principles, integrity requirements, and the company's code of conduct and house rules • Be able to identify potential risks of violation of law, and seek attention of senior management or appropriate authority as necessary 3. Exhibit professionalism • Possess and exhibit a high standard of personal integrity as well as law-compliant and ethical culture in performing one's duties; and • Understand the corruption/integrity challenges that may arise in the work environment, and be able to deal with them properly
Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Develop a law-abiding awareness, gained a practical understanding of the anti-bribery law and common corruption challenges at work, and being capable to deal with them properly • Gain a good understanding of the expected standard of integrity and common ethical challenges at work, and being capable to deal with them properly.
Remark	

Title	Provide support for handling professional ethics and conducts issues
Code	107870L3
Description	This unit of competency applies to supervisors of IT support personnel. Code of ethics are broad guidelines that restricted to certain situation at workplace and cannot be applied to all situation. Hence, when cases are reported it needs to be investigated and handle correctly to ensure that the action is complied with the code of ethics itself.
Level	3
Credit	3

Competency	Performance Requirements
	1. Knowledge for providing support for handling professional ethics and conducts issues:
	
	• Possess good listen and communication skills to understand reported ethical issues and gather related facts
	• Possess people management skills deal with people of different level and different departments
	• Possess detailed knowledge of the organisation's code of ethics
	• Possess detail knowledge of the organisation's guide on professional conducts
	• Understand the importance of professional ethics compliance and effects it has on the organisation
	2. Provide support for handling professional ethics and conducts issues
	
	• Patiently listen to reported professional ethics issue and obtain all relevant facts without drawing any conclusion or judgements
	• Identify the ethical issues from facts by referring to the organisation's code of conduct guidelines and ethics standards, if any
	• Investigate and verify the reported ethical issues
	• Determine the impacts and gravity the issue has on the organisation (reputation, operation, customer and staff) and the offender. Also determine social and legal impacts
	• Identify and weight out all alternatives persons/parties who can resolve the dilemma, including:
	    o Human Resource
	    o Next higher level of authority
	    o Law enforcement
	• Identify the consequences of each alternative
	• Recommend appropriate action in accordance with the organisation guidelines for handling ethical and code of conduct issues, including completing documents
	3. Exhibit professionalism
	
	• Committed to adhere to the industry and organisation's professional ethics and be fair and unbiased when handling ethical and code of conduct issues

Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Understand, collect and investigate the reported ethical or code of conduct issue in accordance with the organisation's guidelines • Identify the true impact the ethical issue or code of conduct had, in respect to the organisation, operation, customer, staff including the offender • Recommend corrective action in accordance with the organisation guidelines after taken into account all relevant facts, weighted the effects and consequences, after a breach of ethics or code of conducts

Remark	

Title	Implement "clean" business practices, good controls and integrity management
Code	107871L3
Description	This unit of competency is applicable to managerial staff and staff entrusted with supervisory role involved in ICT functions, e.g. purchasing, contract management, staff management. Practitioners should be capable of implementing "clean" business practices, proper controls and good integrity management in day-to-day operations, and helping their organisations adopt and put in place relevant practices and measures.
Level	3
Credit	3
Competency	Performance Requirements 1. Knowledge of anti-bribery legislation, risk areas in the industry and basic principles of "clean" business practices, internal control and good integrity management: • Understand the key legal requirements of the Prevention of Bribery Ordinance and what company staff should know about it, and "clean" business practices in line with the requirements • Understand and be aware of the importance of staff integrity issues • Understand the key elements of a good integrity management programme for an organization and how to implement it • Understand the risks of corruption/malpractice in various common functions/processes in the industry • Understand the principles of good internal control and preventive measures, and their application to common functions/processes • Understand the role and duty of a supervisor in respect of managing staff integrity, exercising proper supervisory controls and ensuring "clean" business practices in day-to-day operations 2. Implement "clean" business practices, good controls and integrity management • Advise and assist senior management to adopt, and assist the organisation to implement, "clean" business practices, internal controls and integrity management programme (e.g. company code of conduct) • Exercise effective supervision over their staff and day-to-day operations (in respect of ensuring integrity and "clean" business practices) • Respond to integrity issues and challenges, and provide guidance/advice to subordinates/management, and/or assist the organisation, in managing such issues • Inspire upon and set examples for subordinates and other staff on integrity and "clean" business practices • Provide training or coaching to enhance staff awareness of integrity issue and clean business practices 3. Exhibit professionalism • Apply best practices to help implement good integrity management, raise staff awareness of the anti-bribery law and integrity issues, and guide them on such matters
Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Apply knowledge in the basic legal requirements of anti- bribery law • Assist the company in implementing good integrity management; and • Assist the company in adopting and implementing "clean" business practices and basic/key internal controls to mitigate the risks of corruption/malpractice in performing key ICT functions

Remark	

Title	Coordinate application change requests with developer
Code	107872L2
Description	This unit of competency applies to IT support personnel. Many systems are tailor-built due to special features and functions needed and canned packages cannot provide. The development work may be internal or external. As errors are being identified and new functions are required, a single contact point to coordinate with developers is required. This UoC will synonymously use "change request" for either error report and functional change request.
Level	2
Credit	3

Competency	Performance Requirements
	1. Knowledge for coordinating application change requests with developer
	
	• Possess good interpersonal and communication skills for liaising with users and developers
	• Possess basic knowledge of change management concept
	• Possess good knowledge of the organisation's change record system
	• Good teamwork attitude, self-disciplined and resourceful
	2. Coordinate application change requests with developer
	
	• Received change request from user by "change request form"
	   o Verify details of change request and perform initial filtering based on organisation's change control procedure
	   o Record the change request into internal record system with a change control ID number
	   o Forward to supervisor to approve the change request or error report
	   o Agree with change controller and allocate the level of priority for the change request
	   o Forward change request to developer with indication of priority level
	• Liaise new change request with developer
	   o Gather details of change request for developer
	   o Acquire assigned reference details from developer and timeline for completion of work
	   o Update developer given reference details to corresponding change request
	• Regularly monitor change request and its status. Contact developer for status may be required
	• Liaise with users relating to change requests, such as:
	   o Provide status of change such as: accepted, rejected, ref. ID, etc.
	   o Developer need for extra details related to the change request
	   o Notify change request has been completed by developer
	   o Acquire feedback to determine whether the change request completed to user's expectation
	• Regularly monitor change request and its status
	   o Update change request records with status of different stages of processing
	   o Request change controller to close the change request on work completion when user is satisfied with delivered changes
	3. Exhibit professionalism
	
	• Apply industry best practices for change management process and follow the organisation change control procedures to ensure all change control records are well maintained and updated

	• Take responsibility and accountable for coordination work and be impartial between users and developers regarding change requests
Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Understand change request made by users and can accurately record it into the organisation's change control record system • Convey adequate details of change request to developer that enable them to accurately assess the viability and plausibility of performing requested changes and can give an estimate of completion time • Monitor progress of change requests systematically in such a manner where important/critical change requests demand more frequent follow up and less critical ones are reported on scheduled dates
Remark	

Title	Install and configure Apps on client devices
Code	107873L2
Description	This unit of competency applies to IT support personnel who are responsible for installing software applications (Apps) on different computing clients such as: personal computers (PC), notebooks, tablets and smartphones. When installing Apps for user some minimal training on use of the Apps would be needed
Level	2
Credit	3

Competency	Performance Requirements
	1. Knowledge for installing and configuring Apps on client device:
	
	• Possess good troubleshooting skills
	• Possess basic training skills
	• Possess basic knowledge of operating different computing clients
	• Possess good knowledge of installing software application
	• Possess basic knowledge of reading technical manual and following software installation and configuration instructions
	• Possess basic knowledge of the organisation health and safety guideline
	2. Install and configure Apps on client devices
	
	• Comprehend the software installation request from supervisor or user
	• Prepare for installation
	    o Comprehend a basic function overview, installation details and configuration details of the Apps
	    o Obtain installation media of the Apps
	    o Ensure the client devices conform to the minimum hardware requirements and sufficient storage space
	    o Locate or purchase the Apps' installation key or license, if required
	• Prepare the installation media
	    o For PCs and notebooks, mount installation media
	    o For tablets and smartphones, locate the Apps in the "market store" of the mobile platform. Example; IOS = App Store, Android = Play store, etc.
	• Follow the installation instructions of the Apps during the installation
	• Enter the license or installation key, if required
	• Configure the Apps with required settings that complied with the organisation security policy. Extra care should be paid to mobile Apps to avoid giving unnecessary authorisation to access device and personal information
	• Perform simple test to ensure the Apps can function normally in the expected manner. Troubleshoot any error messages during the installation and find rectification solutions before restarting installation
	• Complete internal documents and record configuration setting in accordance with the organisation's procedure
	3. Exhibit professionalism
	
	• Possess services attitude with desire to assist users with problems
	• Follow organisation safety guidelines and procedures when performing installation and configuring Apps on client devices

Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Perform preparation for installation process

		• Complete installation and configuration of Apps on the client device that meets the need of user and complied with the organisation security standards • Provide sufficient instructions or training to the user to enable them to operate the App with minimum problem
Remark		

Title	Perform application configuration
Code	107874L2
Description	This unit of competency applies to IT support personnel who are responsible for supporting application configuration on different computing clients. The configurations are performed either at initial application installation or when there is a changed need requested by users or organisation wide. Configuration can be of different level ranging from simple cosmetic adjustment match individual users need to functional and features specific configuration which applied to companywide. For example, all pdf readers must support multi-language (English and Chinese) and has commenting functions.
Level	2
Credit	3

Competency	Performance Requirements
	1. Knowledge for performing application configuration
	
	• Possess good reading skills to understand technical manual and follow software installation and configuration instructions
	• Possess basic training skills
	• Possess basic knowledge of operating different computing clients
	• Possess good knowledge of installing software, configuring applications and script programming
	• Possess basic knowledge of application testing
	2. Perform application configuration
	
	• Comprehend the application configuration requirement from work order or from user request
	• Review vendor documents to determine whether the required changes/configuration is available and can be performed on the application
	• Comprehend from appropriate technical documents, from vendor or other sources, to determine how configuration is performed on the application, such as:
	    ○ Menu driven within the application
	    ○ Direct editing of configuration file
	• For menu driven configuration method, locate which menu and what option settings
	• For configuration file settings method, identified name of configuration file and used appropriate editor to add/change settings on the file which configures the functions required by the user
	• After completed the configuration, perform appropriate tests to ensure the application functions are performing as required
	• Where necessary, provide operation instructions and/or provide basic tutorial to users on usage of configured functions
	• Complete internal documents and record configuration setting in accordance with the organisation's procedure
	3. Exhibit professionalism
	
	• Committed to ensure completed work is free from error and function as required
	• Follow organisation safety guidelines and procedures when performing configuration work

Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to:

	- Fully comprehend the configuration requirements and are well prepared for the configuration work, identified of where, and how to make the required configuration settings on the application - Perform the required configuration and satisfactorily test the application before release for general use - Complete the after configuration document in accordance with the organisation procedure and provide sufficient instructions or coaching to users on use of configured functions
Remark	

Title	Troubleshoot application problems
Code	107875L3
Description	This unit of competency applies to IT support personnel who are responsible for application support. When users encounter application issues they request help from support team. The support personnel general responsibility includes troubleshoot and collect necessary information to be forwarded to application developer or vendor when reporting the problem. Additionally, the support personnel will provide advice and/or attempt to adjust configuration (system or application) to enable the application function or to bypass the problem and enable the user to continue with work.
Level	3
Credit	3

Competency	Performance Requirements
	1. Knowledge for troubleshooting application problems
	
	• Possess good interpersonal skills that can communicate effective with different level of users
	• Possess good application troubleshooting skills
	• Possess basic knowledge of organisation's application support guidelines and procedure
	• Possess basic knowledge of the internal problem recording system
	2. Troubleshoot application problems
	
	• Patiently listen to user or read problem report on symptoms of application problem and explain the actions will be performed and reason for the actions
	• From internal records, from user, or from the client system, gather as much as possible on details relating to the problem application, including but not limited to the following:
	   o Type of application
	   o Hardware, environment and compatibility requirement
	   o Configuration details
	   o Functions and features of the application
	   o Version/release number
	• Collect various messages related to the application problem, include:
	   o System log
	   o Application log
	   o Error messages from the application
	• Reconstruct the problem and analyse from available information to determine cause of problem, such as:
	   o Installation and configuration problem
	   o Startup problem
	   o Insufficient system resource
	   o Incorrect input or output
	   o User incorrect operation
	• During the recreation of the problem, record all actions performed, and/or capture all input and output, which will be forwarded to the application developer or vendor to assist application correction and for further detail analysis when required
	• Attempt to correct or bypass the problem by performing some of following actions:
	   o Reconfigure the application
	   o Uninstall and re-install the application
	   o Adjust system resource for the application
	• Perform simple tests to ensure the problem is corrected or bypassed before return it for user to use

	• Report the problem to application developer or vendor and forward the collected packaged details that include error messages, logs details, input and output details • Complete the internal record keeping procedure in accordance with the organisation guidelines and requirements 3. Exhibit professionalism • Possess customer services attitude with desire to assist users with problems
Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Communicate effectively with user to understand the issues of the application and collect sufficient information to re-create the problem • Identify the cause of the application problem and follow the organisation procedures and guidelines to collect sufficient details that can be used for further analysis and can be forwarded to application developer or vendor to assist with correction of the application • Provide suitable advice or perform appropriate setting corrections to application or system to enable it to continue function so that the user can continue with his/her work
Remark	

Title	Install and configure email clients
Code	107876L2
Description	This unit of competency applies to IT support personnel who are responsible for installing email clients on different computing clients. Computing clients can be personal computers or mobile/smart devices. For the context of this UoC, email clients refer to specialised email application and not browser based webmail which normally does not require installation on the user's device. An organisation would normally standardise the email client being used, but selection of email protocols (SMTP, POP, IMAP, MAPI) may differ to suit to different work styles (on one device or more than one device) and types of email servers.
Level	2
Credit	3

Competency	Performance Requirements
	1. Knowledge for installing and configuring email client:
	
	• Possess good troubleshooting skills
	• Possess basic training skills
	• Possess good knowledge of operating different computing clients
	• Possess detailed Knowledge of installing software application
	• Possess basic knowledge of the organisation health and safety guideline
	• Possess good knowledge of common email protocols, such as SMTP, POP, IMAP and MAPI
	
	2. Installing and configuring email client
	
	• Comprehend the user's working style and agree with user on which is the best email protocol to use
	• Prepare for installation
	    o Obtain installation media of the email client App
	    o Acquire email server configuration details including:
	        • Types of email protocol available
	        • Secure connection setting
	        • Port numbers
	• Prepare the installation media
	    o For PCs and notebooks, mount installation media if extern or copy the installation program to the device
	    o For tablets and smartphones, locate the email App from the device's "Marketplace"
	• Start the installation of email client, follow the installation instructions during the installation
	• Enter the license or installation key, if required
	• Configure the email client with appropriate protocol to access and view email on the email server
	• Test the email client with user's logon setting. Troubleshoot and rectify connection and access issues
	• Provide instructions or training to user on how to logon and use the email client
	• Complete internal documents and record configuration setting in accordance with the organisation's procedure
	
	3. Exhibit professionalism
	
	• Possess services attitude with desire to assist users with problems

	• Follow organisation safety guidelines and procedures when performing installation and configuring software applications on client devices
Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Select and advise the user on best protocol to use based on user's working style • Install and configure email client on user's client device successfully that can enable the user to send/receive emails and the procedure follows the organisation's standard guidelines • -Pprovide sufficient instructions or training that enable the user to use the email client with minimum trouble in addition to logon and access their email service
Remark	This UoC is related to 107873L2 "Install and configure Apps on client devices"

Title	Detect and protect against email spam
Code	107877L2
Description	This unit of competency applies to IT support personnel who are responsible to support users with email issues. This UoC concerns support of email spam which is one of the biggest causes of email security risks. Support personnel will assist users when they encounter problems caused by spam emails, such as clearing problems like virus and spyware from the client machines, setting the email client to detect, filter and block spam email. Additional and more importantly they need to provide friendly advice on how to spot malicious email.
Level	2
Credit	3

Competency	Performance Requirements
	1. Knowledge for detecting and protecting against email spam
	
	• Possess good troubleshooting skills
	• Possess basic training skills
	• Possess detail knowledge of email client applications
	• Possess good knowledge of Internet security
	2. Detect and protect against email spam
	
	• Work with users to understand the nature of effect the spam email, including, unusual activities on their system, problems and symptoms which user is experiencing
	• Apply troubleshoot techniques to determine the type of spam email, including but not limited to:
	    o Phishing and spoofing
	    o Malicious attachments
	       ▪ Virus and malware
	       ▪ Trojan horse
	       ▪ Malicious macros embedded in documents
	    o Scams
	• For malicious type, follow the organisation guidelines to apply damage control procedures to limit damages, such as stopping spreading of virus
	• For "social engineering" type, follow the organisation security guideline to escalate the incident to supervisor (see Section 8 "Remarks") and advice and assist users to check if their personal identities and financial has been compromised
	• Collect evidence of spam email for records and apply removal and cleaning/recovery procedures to remove email spam email
	• Perform update of email client application on users' system and set filtering function to remove future junk/spam emails
	• Provide some instructions and tutoring tips on spotting malicious spam emails, particularly on dealing with attachments
	3. Exhibit professionalism
	
	• Fully updated with Internet and email security
	• Apply industry best practices to secure the organisation from email attacks

Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Detect the type of damages caused, if any, by the spam email • Take suitable actions and provide suitable advice to user to limit damages caused by the spam email

	• Protect the users' system from receiving further spam email by configuring or adding functions into the email client and provide adequate and effective instructions or tutoring to the users
Remark	Please refer to 107860L1 "Perform next level escalation" for detail actions of escalation

Title	Resolve email problems
Code	107878L3
Description	This unit of competency applies to IT support personnel who are responsible for email client support. Many organisations and users are heavily dependent on using email for business and personal communication. In an organisation daily operation, users can experience many different issues, ranging from unfamiliar with functions of the email client to server connection problems. Because of the importance of email, support staff is expected to be able to resolve the problem quickly and immediately. This UoC will concentrate in the support of email client issues.
Level	3
Credit	3

Competency	Performance Requirements
	1. Knowledge for resolving email problems
	
	• Possess good communication and interpersonal skills
	• Possess good email client troubleshooting skills, including use of telnet
	• Possess basic training skills
	• Possess good knowledge of popular email clients
	• Possess good knowledge of installing and configuring email clients
	• Possess good knowledge of common email protocols, such as SMTP, POP, IMAP and MAPI
	
	2. Resolve email problems
	
	• Politely and patiently to comprehend user report on email client issues and symptoms
	• Access the email client through remote or on premise access to troubleshoot the email client, including but not limited to the following:
	    o Internet connection
	    o Email server configuration
	    o Account configuration
	    o System and email client application logs
	    o Email box limits
	    o The size limits of each email
	    o Browser compatibility issue, for webmail
	• Identify area of possible issues and determine whether a solution exists from:
	    o The internal Trouble Ticket System (TTS)/Problem log
	    o Internet searching
	    o Email client's vendor
	    o Colleagues
	• Proceed to rectify the issue, including but not limited to the following:
	    o Reconfigure setting to the email server
	    o Reconfigure email account login details
	    o Clear email box to make space
	    o Adjust browser settings for web application email client
	    o Uninstall and reinstall the email client
	    o Provide alternative method of emailing, such as: change from installed email client to use web based email client and vice versa
	• Provide explanation on cause of issue and the rectification details to user. Also provide some instructions or tutoring on proper use of the email client
	• Complete internal documents including create/update TTS/Problem log entries in accordance with the organisation's procedure

	3. Exhibit professionalism • Possess service attitude with desire to assist users with problems • Be security conscious and always advise users to change their account password after the completion of work • Follow organisation guidelines and procedures when dealing with users
Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Use various troubleshooting techniques to identify issues and be able to escalate or seek help from colleagues when needed help • Resolve the issues or provide alternative solution to the users so that the users can continue to communicate via email • Complete the documents and record the problem in accordance with the organisation standards and procedures
Remark	

Title	Build a small wireless LAN
Code	107879L2
Description	This unit of competency applies to junior IT personnel who are involved with construction of the organisation's network infrastructure. The main duties include installing, configuring of small wireless local area network (LAN) as well as performing user training on the use of the wireless LAN. However, during the planning and network design and sourcing of equipment for the wireless LAN he/she may be required to provide advice and assistance.
Level	2
Credit	3

Competency	Performance Requirements
	1. Knowledge to build a small wireless LAN:
	
	• Possess good communication and interpersonal skills
	• Possess good knowledge of basic training skills
	• Possess good knowledge of different network and wireless security risks
	• Possess good knowledge of wireless LAN components and their functions
	• Possess good knowledge of how to acquire technical manuals on wireless LAN equipment
	• Understand the network needs of users and the organisation
	• Possess good knowledge on use of network testing software
	2. Building a small wireless LAN
	
	• Comprehend and assess the wireless LAN design diagram. Confirm and raise any concerns or suggestions with the designer or supervisor before purchase of equipment or install work. Area where he/she may assist include but not limited to the following:
	    o Evaluate and/or selection of wireless equipment
	    o Advice on any blind spots that affect the wireless signal
	    o Site survey
	• Prepare for installation of wireless LAN
	    o Identify the location of wireless router/Access Point and can be connected to the wired local network or to Internet service provider
	    o Verify power availability for the wireless router
	    o Verify Access Point (AP) has mounting space and signal are not obstructed that reduced transmission efficiency
	    o Acquired network settings
	    o All required equipment have been checked, verified working, and installation manuals are available
	• Install and configure the wireless router
	• Perform a wireless coverage test. Install wireless extension device to increase network coverage and remove blind spots, if needed
	• Configure security settings that conform to the network design and the organisation security policies
	• Install and configure wireless LAN cards on personal computers or join mobile client and smartphone to the wireless LAN then perform the following tests:
	    o Test connection of the wireless network with user equipment to ensure general compatibility and access
	    o Perform speed tests to ensure client connection is of expected performance
	    o Perform security tests to ensure only authorised clients can connect to the wireless network

	- Label all wireless LAN equipment in accordance with the designed infrastructure plan/diagram - Provide instructions sessions and/or tutoring to users on use of wireless network, topics include: - Pairing with designated Service Set Identifier (SSID) - Logon arrangements - Use of wireless LAN equipment - Document all installation activities and record configuration and security settings details in accordance with the organisation's guidelines and procedures 3. Exhibit professionalism - All installation activities and preparation of documents were performed in accordance with organisation guidelines and standards - Always protect the organisation against unauthorised wireless connection and apply industry network security best practices - Follow the organisation's occupational health and safety guidelines and procedures when installing with network equipment
Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: - Perform the necessary preparations before the installation of wireless LAN - Install, configure and test the wireless LAN and equipment in accordance with the organisation's requirements and standards - Provide sufficient and satisfactory training to users that enable them to access the organisation network resources
Remark	

Title	Install and configure network components/devices
Code	107880L2
Description	This unit of competency applies to support personnel who install and configure network components or devices in a small internal Local Area Network (LAN) environment. A small network would comprise of Internet connection with wireless and wired Internetworking devices such as switches, routers, wireless LAN Access Points (AP).
Level	2
Credit	3

Competency	Performance Requirements
	1. Knowledge for installing and configuring network components/devices:
	
	• Possess basic network troubleshooting skills
	• Possess good knowledge of system and network monitoring equipment
	• Possess good knowledge of internetworking devices
	• Possess good knowledge of network concepts, such as:
	    o Network types
	    o Types of cables and distance limits
	    o Wireless LAN
	• Possess good knowledge of the TCP/IP protocol
	• Possess basic knowledge of procedures for handling electrical devices
	2. Installing and configuring network components/devices
	
	• Comprehend the installation requirements including:
	    o Types of network component/device
	    o Verify location is suitable for the installation work
	• Prepare for installation work
	    o Assess network component/device power and cabling needs
	    o Verify location is suitable for the installation
	    o Acquire the network component/device
	    o Acquire technical manuals and comprehend the installation and configuration instructions
	    o Acquire network configuration information for the network component/device
	• Perform the installation of network component/device complying to the organisation and manufacturer's procedures
	• Configure and test the network component/device to ensure it complies with the organisation's network requirement
	• Clean installation site and return equipment to appropriate location
	• Document the installation and configuration according to the organisation guidelines and standards
	3. Exhibit professionalism
	
	• Adhere to the organsiation's occupational safety procedure
	• Well converse with industry's networking best practices

Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Be well prepared for the installation work • Follow the work order and install the network component/device according to the manufacturer and the organisation procedures • Perform post installation procedures satisfactorily and well document the configuration details and installation work according to the organisation standard procedures

Remark	

Title	Setup content sharing on server
Code	107881L2
Description	This unit of competency applies to support personnel who are responsible for administering network content sharing on the organisation server to users. He/she would follow work order to setup required directory/folder on the server to permitted users to manage contents for sharing. Once the shared resources have been set some instructions or training in usage of the shared functions would be provided.
Level	2
Credit	3

Competency	Performance Requirements
	1. Knowledge for setup content sharing on server
	
	• Possess basic knowledge of common network servers
	• Possess basic knowledge of the server file system
	• Possess basic knowledge of network and content security
	• Possess good knowledge of administering content sharing on server
	• Possess basic knowledge of common network file sharing protocol, including:
	  o Server Message Block (SMB)
	  o Common Internet File System (CIFS)
	  o File Transfer Protocol (FTP)
	2. Setup content sharing on server
	
	• Comprehend work order to determine the requirements for setup of content sharing on the server, including but not limited to the following:
	  o Folder name (physical folder and shared folder name)
	  o Folders size
	  o Owner of the folder
	  o User and user group name and access rights (read only, read/write, etc.)
	  o Security requirements
	• Create a new directory/folder with the required name and set quota size according to the organisation's policy, if any
	• Configure directory/folder with required access rights to allow appropriate users to access, download, upload file contents
	• Configure security settings, including:
	  o Encryption of file sharing connection
	  o Password protections
	• Perform simple tests, including:
	  o Shared folder is discoverable across the network
	  o User accessible
	  o Contents can be maintained (upload, delete) by authorised user
	  o Content is protected from unauthorised user
	• Provide instructions and/or tutoring to users on usage of the network sharing functions
	3. Exhibit professionalism
	
	• Committed to serve users and protect the organisation servers

Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Fully comprehend the work order and able to clarify ambiguous requirements • Setup the content sharing on the server in accordance with the work order requirements and the organisation's standards and policies

	• Provide clear instruction or training to users on usage of the network shared functions
Remark	

Title	Install and configure client/server application
Code	107882L3
Description	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 "loosly 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:
	        o Identify what installation options are required from work order
	        o Identify hardware requirement (i.e. server and client side)
	        o Identify software requirement (i.e. database, middle ware, etc.)
	        o Identify network requirements
	        o Identify security requirements
	        o Identify what data migration is required, if any
	    • Preparing for installation
	        o Upgrade hardware of server and client device, if required
	        o Acquire the client/server application installation media
	        o Familiarised with the client/server application installation instructions from vendor documents
	        o Acquire associated settings for the client/server application, such as:
	            ▪ IP address of the server and client
	            ▪ Network settings
	            ▪ Authorised access account settings
	        o Acquire all necessary technical manuals
	        o Backup the server and client systems
	        o 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
	        o Configure security and access settings to allow client to connect
	        o Undertake restore or migration of data, if required
	        o Perform appropriate tests
	    • Install and configure client side of the client/server application as required by the work order
	        o Configure security setting to enable access to the server side
	        o Configure appropriate functions of the application
	        o 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	

Title	Configure WAN connection
Code	107883L3
Description	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:
	   o 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
	   o Acquire and install router as per required by manufacturer
	   o 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

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	

Title	Troubleshoot network issues
Code	107884L3
Description	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
	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
	    o Inspect for loose cabling on the network devices, network clients, and network components. Reconnect and secure cables
	    o Use cable testing equipment to test cable to ensure it is still functioning
	• For wireless connection issues
	    o 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
	    o Acquire network settings from network administrator
	    o Verify the software configuration setting matched the network settings. Reconfigure if necessary
	• For network component issues
	    o 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
	    o Verify the device configuration setting is correct
	    o 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	

Functional Area - Network Support

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	

Title	Create and maintain user accounts on server
Code	107885L2
Description	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
	2. Create and maintain user accounts on server
	
	• Determine the needs of the accounts on server, such as:
	  o The role of the user (user, administrator, operator, etc.)
	  o Which server, if there are more than one
	  o Personal folder for the user
	  o Access to server resources
	  o Application settings
	  o 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:
	  o Security role of the account
	  o Directory and file permissions
	  o Password length
	  o 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:
	  o Accounts involved with unusual activities
	  o Attempt to access unauthorised resources
	  o Accounts locked out
	  o 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	

Title	Configure user access control on server
Code	107886L3
Description	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:
	    o Administrator
	    o Backup operator
	    o Application administrator
	    o 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:
	    o Local logon
	    o Internet access
	    o 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:
	    o Printers
	    o Folders
	    o Files
	    o 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

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	

Title	Administer basic network security
Code	107887L3
Description	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
	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	

Title	Administer system security
Code	107888L3
Description	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:
	    o List of authorised personnel/users that can access the system
	    o Level of access/tiered access, or what each user is allowed and not allowed to do on the system
	    o Access control methods, or how users will access the system (user ID/password, digital card, biometrics)
	    o System setting and application needed to strengthen the system and how weaknesses are handled
	    o Which system required system backup and what type of backup procedure to apply
	    o Network security settings and configurations
	• Install the required security application, such as:
	    o Antivirus and spyware protection applications
	    o Personal firewall
	    o Malware protect application
	• Configure and set remote access and support function according to the organisation guideline and procedure
	• Configure network and firewall
	• 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
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	

Title	Administer basic website security
Code	107889L3
Description	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:
	    o Website functionality
	    o Access requirement of transactions, visitors and users
	    o 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	

Title	Administer perimeter firewall
Code	107890L3
Description	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:
	    o Create new rules
	    o Amend existing rules
	    o 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	

Title	Strengthen workstation protection
Code	107891L3
Description	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
	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	

Title	Maintain inventories of equipment/software
Code	107892L1
Description	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:
	   o Computer systems
	   o Monitors
	   o Word processing software license
	   o 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:
	   o Reference/Identification number
	   o Description
	   o Purchased date
	   o Supply details
	   o 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	

Title	Implement system maintenance procedures
Code	107893L2
Description	This unit of competency applies to IT personnel who are responsible to implement the organisation system maintenance procedures. An organisation's system maintenance procedure can be simple or complex depending on the size of IT support. The maintenance work can be outsourced or performed internally. This UoC concerned in-house system maintenance competencies and of normal planned scheduled type rather than ad-hoc or emergency type. Some organisation's procedures have been developed to meet security and compliance requirements which the practitioner must be aware of
Level	2
Credit	3

Competency	Performance Requirements
	1. Knowledge to implement system maintenance procedures:
	
	• Possess good communication and interpersonal skills
	• Possess good system troubleshooting skills and recognise common symptoms of hardware and software
	• Understand computer maintenance and preventative maintenance concepts
	• Possess basic knowledge of the organisation's system maintenance procedures and guidelines
	• Understand the importance of system maintenance
	• Possess basic knowledge of Occupational Safety procedures
	
	2. Implementing system maintenance procedures
	
	• Comprehend the organisation's system maintenance procedure and directives
	• Review systems past maintenance logs and priorities for system to be scheduled for maintenance and categorised into different types of maintenance to apply, such as monthly, quarterly or yearly
	• Follow the organsiation's procedure requirement to notify all stakeholders and users on the maintenance work and duration of work
	• Prepare for maintenance work
	   o Acquire and collect components/parts for the maintenance work, including
	      ▪ Tools kit and cleaning equipment
	      ▪ Testing tools and applications
	   o Perform a backup image of the system for recovery purpose
	• Request all users and transaction processing applications to exit the system
	• Perform maintenance work in accordance with the organisation maintenance procedure, including but not limited to the following:
	   o Use appropriate tools to check hardware components' performance, such as hard disks, USBs, network cards, CPU fan, CMOS battery, etc.
	   o Check system versions, and perform the necessary system updates
	   o Check system bios or firmware versions and perform update, if necessary
	• Perform internal cleaning of the system, including the power supply unit, fans, the motherboard and the case unit
	• Replace faulty components/parts based on test reports and recommendations. If hard disks are replaced, recover the system from backup image. Handle old disks in according with the organisation procedure and policy. Disk sanitisation procedure need to be followed
	• Perform cleaning of work area after the system maintenance work

	• Document and update maintenance record according to the organisation standards and procedure 3. Exhibit professionalism • Keep abreast with industry best practices for system maintenance and explore better maintenance techniques • Follow organisation safety procedures when performing system maintenance work
Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Follow the organisation system maintenance procedure to perform system maintenance work • Complete the system maintenance work within the announced schedule • Complete all the necessary documents and update of records according to the organisation's standards and procedures
Remark	

Title	Provide support for different operating systems
Code	107894L2
Description	This unit of competency applies to IT support personnel. All IT users that use computing client devices need to operate one of the common operating systems (OS) to manage a variety of computer operations and sharing of computer resources on their computing device. When there are issues, IT support personnel are there to assist. These UOC concerns the basic skills required of these support personnel to assist users when they have problems with their OS. Although this UOC is mainly concerned with desktop/notebook OS but some of the skills may be applied to supporting OS of mobile devices.
Level	2
Credit	3

Competency	Performance Requirements
	1. Knowledge for providing support for different operating systems
	
	• Possess good troubleshooting skills of OS issues
	• Possess basic knowledge of computing hardware, OS, applications and network equipment
	• Understand the association between OS and the client device
	• Able to plan work or follow organisation procedures and guidelines
	• Good teamwork attitude, self-disciplined and resourceful when supporting OS issues
	2. Provide support for different operating systems
	
	• Determine the type of OS that client device is using, such as:
	    o Desktop
	    o Server
	    o Mobile OS
	• Familiar with functions and features of different types of OS, including but not limited to the following:
	    o Managing hardware and software
	    o Resource management and monitoring
	    o Networking
	    o Security
	    o User management and access control
	• Support common OS functions, including but not limited to the following:
	    o Install/upgrade OS
	    o Configure OS, such as network, device, security, shared resources, etc.
	    o Manage user accounts
	    o Perform optimisation/performance tuning
	    o Perform OS Settings
	• Perform updates in accordance to organisation guidelines, such as:
	    o Test updates before installation
	    o Determine if the concerned update is permitted
	    o etc.
	• Use advanced or privileged commands to manage the OS or perform advanced support functions, such as:
	    o Access or make changes to the registry or kernel
	    o Trace network settings
	    o Adjust security settings
	    o etc.
	• Consult colleagues or other sources to find solution, when OS having issues

	• Keep full records and history of OS settings, configuration, updates, etc.
	3. Exhibit professionalism
	• Apply industry best practices when supporting operating systems
	• Follow organisation safety procedures when handling any hardware or equipment during the supporting of operating system process
Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to:
	• Be familiar with common OS features and able to differentiate features of server and client OS
	• Use system commands to troubleshoot common OS issues or access OS privileged setting
	• Follow the organisation guidelines and procedures to keep OS updated
Remark	

Title	Configure desktop client environment
Code	107895L2
Description	This unit of competency applies to IT personnel who follow procedures or work orders to setup work environment on desktop client devices. Desktop client devices include notebook and Personal Computers (PCs). Work environment includes Operating System (OS) with standard and predefined applications.
Level	2
Credit	3

Competency	Performance Requirements
	1. Knowledge to configure desktop client environment
	
	• Familiar with desktop work environments
	• Familiar with installation and configuring of software applications and operating systems
	• Possess good troubleshooting skills
	• Possess good knowledge of application testing and able to setup and perform testing
	2. Configure desktop client environment
	
	• Comprehend the work order to determine what type of devices to be configured and what work environment is required to install and configure
	• Prepare for the configuration of client devices
	    o Obtain installation media of OS and applications
	    o Obtain all the necessary licenses
	    o Backup the client devices
	• Configure network settings to connect to the Internet
	• Patch or upgrade the OS and applications using appropriate upgrade method
	• Configure desktop client, including but not limited to the following:
	    o Configure hardware device
	    o Configure access to organisation network resources
	        • Network domain
	        • Servers
	        • Shared files
	        • Network printers
	    o Configure applications according to business requirements and may be user's working practices
	    o Configure security setting according to business requirement and organisation policies
	• Test the client device to ensure the configured settings are performing as required
	• Label the client device, in accordance with organisation standards, to indicate completed configuration work and ready for use
	• Complete the necessary documents and record the configuration details of the client device in accordance with the organisation's procedures and standards
	3. Exhibit professionalism
	
	• Follow the organisation procedures and guidelines when configuring client devices
	• Always follow the organisation's safety procedures and guidelines when working with computing hardware

Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Comprehend the work order and understand what type of client device client and applications needed to be configured

		- Be prepared for the configuration work and being at a position to "roll back" in the event of reconfiguration from fresh again or simply just restore the original system - Perform the configuration successfully as required by the work order - Complete the necessary documents in accordance with the organisation's standards
Remark		

Title	Perform Operating System installation
Code	107896L2
Description	This unit of competency applies to IT personnel who follow procedures to perform a brand new installation or upgrade of Operating System (OS) on personal computers or server systems. In the context of this UoC, commonly used OS on personal computers (PC) and notebooks are Windows, Linux and Mac OS and server system OS are Windows and Linux. Each hardware device requires only one single OS installed and the installation is performing locally.
Level	2
Credit	3

Competency	Performance Requirements
	1. Knowledge to perform Operating System installation:
	
	• Understand software license requirements and copy rights responsibilities
	• Familiar with installation of software applications and operating systems
	• Possess good knowledge of basic system booting operation and BIOS settings
	• Possess basic knowledge of disk formats and file systems
	2. Performing Operating System (OS) installation
	
	• Prepare for installation
	    o Understand the installation requirements
	    o Acquire appropriate OS license and/or installation key
	    o Acquire the installation media
	    o Prepare matching media player for installation media such as DVD, USB
	    o Verify the hardware complied with minimum requirement of the OS, including but not limited to:
	        ▪ Disk and RAM space
	        ▪ CPU
	        ▪ Graphic card performance
	• When performing brand new installation
	    o Preformat the disk
	    o Define partition size
	• When performing upgrade of existing OS versions
	    o Perform backups of existing system and files for recovery purpose
	• Install all necessary drivers for attached devices
	• Activate the OS with appropriate license or key
	• Perform post installation tasks, including but not limited to the following:
	    o Configure network settings and connections
	    o Perform OS updates with latest service pack and configure auto update according to organisation's policy
	    o For server installation:
	        ▪ Create all user logon accounts
	        ▪ Set user permissions and access rights
	    o For client:
	        ▪ Create login accounts
	        ▪ Join the organisation's workgroup
	        ▪ Set printer functions
	• Perform basic tests to ensure installation and configurations are functioning as expected
	• Document installation and security settings, configuration performed in accordance with the organisation's procedures and standards

	3. Exhibit professionalism • Follow the organisation procedures and guidelines when performing OS installation • Always follow the organisation's safety procedures and guidelines when working with computing hardware
Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Systematically complete the OS installation that meets the user requirement and complied with the organisation standard • Perform the necessary post installation procedures that can set up the necessary environment, such as login accounts, security, network settings • Complete the documents of activities and recording system changes that conformed to the organisation's required standard
Remark	

Title	Restore system or files from backups
Code	107897L2
Description	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:
	    o File name
	    o Date and time
	    o Destination of restore
	    o 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

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	

Title	Monitor server system status
Code	107898L2
Description	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:
	    o Scan system services activities to verify all the required services are active, such as: network services, system services, messaging services, etc.
	    o Study system event log for error or warning, such as system update failure, system rebooted abnormally, etc.
	    o Study system security log for unusual activities, such as a user account tried to login many times, accounts locked out, etc.
	    o Study the server performance monitoring tools to determine various system resource usage, such as CPU, memory, network, storage, etc.
	    o Study application logs for errors and warnings, such as ftp and web server problems, etc.
	    o 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.
	    o Evaluate monitored result. Report, perform appropriate actions, and/or escalate problems in accordance to the organisation's guidelines and procedures
	    o Backup monitoring and event logs for record keeping and/or evidence
	    o 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

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	

Title	Provide help desk support
Code	107899L2
Description	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

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	

Title	Purchase computing hardware/components
Code	107900L2
Description	This unit of competency applies to junior Information Technology (IT) personnel who have been entrusted with the task of purchasing hardware or components for own use or perform the purchase for colleagues. This UoC concerns small purchase but the involved steps can also be applied for larger purchase by following relevant organisation guidelines.
Level	2
Credit	3

Competency	Performance Requirements
	1. Knowledge for purchasing computing hardware/components
	
	• Possess good knowledge of computing hardware and accessories
	• Possess basic knowledge with organisation's procurement procedures and guidelines
	• Possess good knowledge of IT products and trends
	• Possess good knowledge of the ICAC guidelines on Prevention of Bribery Ordinance and Clean Business Practices
	2. Purchase computing hardware/components
	
	• Find 2 or 3 model names of the needed computing hardware/component with similar specification
	• Search and collect reviews of each of the computing hardware/component model name from:
	    o Previous users, friends, colleagues
	    o Internet
	    o Comment from unbiased retailers
	• Create a comparison list of functions/features which is ordered in the most needed functions/features
	• Identify top 2 most suitable items from the comparison list or the quantity indicated by the organisation purchasing procedure
	• Identify suitable suppliers and acquire price quotations
	• Complete recommendation and purchasing documents in accordance with the organisation's purchasing guidelines and procedures. Authorisation from supervisor may be required
	3. Exhibit professionalism
	
	• Strictly follow the organisation's purchasing guidelines/procedures and ICAC guidelines, and exhibit ethics when procuring hardware/components

Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Perform sufficient research to identify suitable products/models and be satisfied it matches the functions/features required • Seek the required number of quotations from suppliers and follow the procurement guidelines of ICAC and the organisation • Correctly follow the organisation guidelines to complete required documents to seek purchase approval from supervisor
Remark	

Title	Perform system backup
Code	107901L2
Description	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:
	    o operate backup software application
	    o 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:
	    o Mount the media
	    o Validate and ensure sufficient space available for backup
	    o 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:
	    o Dismount media from backup device (if needed)
	    o Label the media in accordance with the organisation guidelines
	    o 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	

Title	Perform fundamental data centre operations
Code	107902L2
Description	This unit of competency (UoC) applies to operational personnel who are responsible to operate the key components of a data centre. The concerned personnel will need to handle various aspects of the data centre such as power, cooling, security, cabling, safety etc. so as to ensure a high-available centre. This UoC also addresses the key operations and maintenance aspects about a data centre.
Level	2
Credit	2

Competency	Performance Requirements
	1. Knowledge to operate data centres
	
	• Possess basic knowledge about a data centre or facilities environment
	• Possess basic knowledge to name and apply various industry standards
	• Possess the skill to identify the components that are important for high availability of a data centre
	• Possess the awareness about the necessity and various technologies for:
	   o Uninterruptible power supply (UPS)
	   o Fire suppression
	   o Cooling
	   o Monitoring systems
	   o Cabling standards, etc.
	• Possess good inter-personal skills to work with people at different levels, including:
	   o Supervisors
	   o Colleagues
	   o Equipment and facilities suppliers, etc.
	2. Perform fundamental data centre operations
	
	• Assist in appropriate data centre sites and buildings selection
	• Assist in acquiring various components and supporting facilities for data centre setup, such as:
	   o Raised floor and supporting ceiling
	   o Lighting
	   o Power infrastructure
	   o Electromagnetic fields
	   o Equipment racks
	   o Cooling infrastructure
	   o Water supply, etc.
	• Participate in the design and planning for the data centre network infrastructure:
	   o Work according to requirements such as:
	      ▪ Network monitoring system requirements
	      ▪ Building-to-building connectivity, etc.
	   o Follow standards such as:
	      ▪ The Copper and Fiber cable technology and standards
	      ▪ The ANSI/TIA-942 cabling hierarchy and recommendations, etc.
	   o Make considerations for:
	      ▪ System testing and verification
	      ▪ Storage area network (SAN) cabling, etc.
	• Carry out routine monitor and precaution tasks, such as:
	   o Maintain fire detection system and follow standards for fire suppression

	○ Capture various total flooding fire suppression techniques and systems ○ Maintain water leak detection systems ○ Monitor status of the Environmental Monitoring System (EMS) and Building Management System (BMS) systems, if installed - Ensure operational security and safety practices, including: ○ Data center security layers ○ Physical, infrastructure and organisational security ○ Safety measures and essential signage, etc. - Perform miscellaneous related activities, such as: ○ Choose a labelling scheme and perform labelling practices, such as cable labelling ○ Setup proper documentation policies and procedures ○ Carry out cleaning practices for the data centre ○ Record mean time between failures (MTBF), mean time to recover (MTTR) information, etc. 3. Exhibit professionalism - Always exhibit loyalty to the work attitude - Apply industry best practices for data centre operations and being up-to-date with the latest technology trends - Always stick to all established procedures and guidelines while at work
Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: - Describe all components that are important for high availability in a data centre and how to setup the data centre - Demonstrate the various technologies for data centre operational tasks - Setup effective data centre monitoring and ensure proper security measures - Assist in designing a highly reliable and scalable network architecture
Remark	

Title	Perform basic system administration
Code	107903L3
Description	This unit of competency applies to support personnel who follow a systematic procedure to perform regular system administration in an organisation. Basic system administration tasks include but not limited to setup, apply and record security access, installed and software licenses, perform system backup and archives, configure network and operating system settings, perform Operating System (OS) and application updates or patches, monitor available resources (disk, CPU, etc.), system boot and shutdown, etc.
Level	3
Credit	3
Competency	Performance Requirements 1. Knowledge to perform basic system administration: • Possess the knowledge of software license requirements and copy rights responsibilities • Possess good knowledge of system functionalities • Possess basic knowledge of the organisation's backup requirements and procedures • Possess good knowledge of the organisation's security requirements and procedures • Possess the knowledge to operate administration tools and understand logs and system messages • Understand the organisation's inventory and recording system • Possess good knowledge of system programming with scripting languages • Possess basic problem solving skills 2. Perform basic system administration • Organise and group all basic system administration tasks in order of priority, such as: daily, weekly, monthly, occasionally • Identify repetitive task that can be automated and use suitable tools or develop simple scripting programs to perform the tasks, such as moving standard file, auto shutdown or reboot, auto backup, start system scan and save reports, etc. • Schedule and perform manual administration tasks to completion • Verify the tasks have been completed satisfactorily. Investigate and resolve any problematic tasks and re-do the tasks. Investigate any unusual security activities and take appropriate action to secure the system • Follow the organisation guidelines and procedure to document all activities related to each system and record all required information such as licenses, configuration changes, applications installed/removed, last backup date, system patched details, user accounts created/removed, security updates, etc. 3. Exhibit professionalism • Follow the organisation procedures when performing system administration tasks • Follow the industry ethics and good practices for an administrator
Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Systematically completed system administration tasks conformed to organisation standards • Identify and automate repetitive tasks • Complete documents of activities and record system changes that conformed to the organisation's standards
Remark	

Title	Provide support to mobile device users
Code	107904L3
Description	This unit of competency applies to IT support personnel who are responsible for mobile device support to users. As organisations are joining the Bring Your Own Device (BYOD) bandwagon, users will need supporting in the work environment; IT support staff will need to have the necessary skills to support and educate users using mobile devices to access the organisation resources. This UoC concerned on area of general support including but not limited to: setup brand new devices to access organisation resources, assist logon and use of Mobile Device Management (MDM) system, protection of corporate information in event of loss of mobile devices, remote support access and support, change configuration and settings, etc.
Level	3
Credit	6

Competency	Performance Requirements
	1. Knowledge to perform remote support:
	
	• Possess good communication, listening and interpersonal skills
	• Possess remote support skills capable to perform troubleshooting, provide instructions systematically and remote problem solving
	• Possess good knowledge of functions and features of the organisation's MDM system
	• Possess good knowledge of mobile device supported applications
	• Possess good knowledge of common mobile device platforms such as IOS, Android, Blackberry, Windows Phone, etc.
	• Well conversed with the organisation's BYOD guidelines and procedures
	• Possess good knowledge of virtual desktop technology and Virtual Desktop Infrastructure (VDI) for mobile device
	2. Perform remote support
	
	• Listen attentively and patiently to understand the user's reported issues
	• Refer to the Trouble Ticket System (TTS)/problem reporting system to determine if similar issues and/or solutions exist
	• For brand new BYOD mobile devices, follow the organisation guidelines to perform some but not limited to the following tasks:
	    o Ensure user understand, agree and accept the organisation policies, particularly when device is misplaced/lost
	    o Install organisation MDM apps and organisation's standard apps
	    o Install mobile support apps, such as: Teamviewer for mobile, Remoty, GotoAssist, etc.
	    o Configure network access setting such as VPN
	    o Backup device
	    o Turn on remote wipe function of the device
	    o Install anti-virus/malware/spyware app
	    o Create new access accounts on MDM server and test connectivity and accessibility to ensure device is function as expected
	• For troubleshooting or remote support, mobile support application or MDM apps should be used to remote access to the mobile device, to view and change setting, screen capture, direct communicating with user to provide instructions to resolve the issue
	• For misplaced/lost device, evaluate the risk of data loss and assist the user to use "find my phone/device/mobile" function or use MDM apps to trace, lock or wipe the device
	• Provide instructions and/or training to users on mobile devices usage and mobile security to protect organisation data

	• Create a new or update Trouble Ticket (TT)/problem report to record the activities transacted during the support session 3. Exhibit professionalism • Possess customer service oriented attitude • Apply industry best practices for mobile support and being up-to-date with mobile technology trends
Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Set up the users' mobile devices to conform with the organisation's mobile device policies • Use appropriate tools to troubleshoot mobile devices, resolve users experience issues and assist or advice users with correct solutions to resolve issues for providing effective support to users and protect the organisation data in the event of user loss • Take correct actions to protect the organsiation's data in the event where users have lost mobile devices • Provide sufficient instruction or training to users on use of mobile devices that conform with the organisation policy
Remark	

Title	Troubleshoot client device hardware issues
Code	107905L3
Description	This unit of competency applies to IT support personnel who are responsible for providing support for client devices. Client devices ranging from personal computer to smart mobile device could experience hardware issues during its operation and support personnel are requested to fix the issues. This UoC concerns the identification of hardware issues before it can be fixed.
Level	3
Credit	3

Competency	Performance Requirements
	1. Knowledge for troubleshooting client device hardware issues
	
	• Possess good troubleshooting and problem analysis skills
	• Possess good knowledge of operating client devices
	• Possess good literacy skills for reading technical manuals of client devices
	• Possess good knowledge of the organisation's procedures for troubleshooting client devices
	• Possess basic knowledge of hardware protection procedures, such as use anti-static straps, etc.
	• Possess basic knowledge of the organisation health and safety guideline
	2. Troubleshoot client device hardware issues
	
	• Comprehend symptoms, if any, prior issues appeared from problem report and/or discussion with user. For example:
	   o Nothing came on when power button pressed
	   o Blank screen but CPU unit appears to be running
	   o System running very slow and continuously rebooting or hanged
	   o System not responding to mouse and keyboard
	• Review maintenance records of the device, to determine if maintenance work has contributed or caused the issues
	• Prepare for troubleshooting:
	   o Acquire all necessary technical and user manuals
	   o Acquire tools to open the client device and tools for troubleshooting
	   o Acquire device components or spare parts
	• Analyse and formulate a troubleshooting plan
	• Without opening to inspect the inside of the client device, perform checks for loose connections, power sockets, battery, display device, etc.
	• View the BIOS error message display code or listen for the number beeps sounded and verify the given code with technical manuals to identify BIOS detected error. For example:
	   o 1 = Loose memory module
	   o 2 = CPU error repair/replace mother board
	   o 3 = display memory error repair/replace display card
	• Next stage of checking is to verify connected components have not affected the functioning of client device, such as:
	   o Keyboards/mouse (swap with a known working component)
	   o Battery low power on mobile device (swap with a fully charged battery)
	   o Hard disk failure (listen for unusual noise)
	   o Power supply unit failure (verify cooling fan is functioning and/or system light is on)

	- For intermittent issues, such as "system hang" or "randomly rebooting" under heavy system work load, identify cause of issue using combination of techniques, including but not limited to the following: - System log messages - Reproduce the issues with monitoring tools - Incorrect BIOS settings - Overheating components - Purpose-built hardware analysis device - For mobile device, once verified it is not battery problem and still cannot be started, return the devices to vendor who will use manufacture's hardware problem analysis devices to identify the issues - Once the cause of issues have been identified, formulate a rectification action plan and clean the work area - Document and record the findings in accordance with the organisation procedures and standards 3. Exhibit professionalism - Follow organisation safety guidelines and procedures when performing troubleshooting of client devices
Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: - Prepare well with troubleshooting work, having all the required tools and manuals for use during the troubleshooting process - Plan the troubleshoot work and systematically perform the troubleshooting to identify the issues or cause of issues - Follow the organisation safety procedures during the troubleshooting process
Remark	

Title	Troubleshoot Operating System issues
Code	107906L3
Description	This unit of competency applies to IT support personnel who are involved with supporting Operating Systems (OS) in an organisation. An OS is basically a very large and complex program that interfaces between the hardware and applications. When the OS is being used its design and programming issues will surface and support personnel will need to minimise the effects on the user. This UoC concerns mainly on troubleshooting common OS issues in desktop environment.
Level	3
Credit	3

Competency	Performance Requirements
	1. Knowledge for troubleshooting Operating System issues
	
	• Possess good communication and literacy skills for handling user and/or comprehending documents (technical manual, user manual, problem report, etc.)
	• Possess good OS supporting skills, including system scripting
	• Possess good troubleshooting skills
	• Possess basic knowledge of computing hardware, Operating System, applications and network equipment
	• Possess the knowledge to plan work or follow organisation procedures and guidelines
	• Possess good knowledge of OS troubleshoot tools
	2. Troubleshoot Operating System issues
	
	• Comprehend the issues and symptoms of the OS issues from the problem report or from user and plan how to troubleshoot the OS issues
	• Backup the computing system before attempting to troubleshoot issues. The backup can be used to restore the computing system to before troubleshooting activities state
	• Attempt to reproduce the issues that were reported, and collect as much information as possible for problem analysis, such as: on screen error message, event/system logs, input activities, etc.
	• For cases when computing system cannot boot, the hard disk and/or the BIOS must be troubleshot and corrected before being able to troubleshoot OS issues. Areas to troubleshoot include but not limited to the following:
	   o Disk for damaged disk
	   o Bad sectors
	   o Corrupted boot partition
	   o Corrupted master boot record
	   o Incorrect boot priority setting in BIOS or loss of BIOS settings
	• Once the computing system is booted, additional troubleshooting tool may be installed to help diagnose the following common causes of OS issues to be troubleshot, include but not limited to:
	   o Install/upgrade issues
	   o Configuration setting (network, security, etc.)
	   o Connectivity (client/server, VPN, etc.)
	   o Device drivers
	   o User setting and access permissions
	   o Performance
	   o Application compatibility and allocation of resources
	• Formulate solutions for correcting OS issues, may require to consult colleagues or other sources, to rectify the OS having issues

	• Apply solution to rectify OS issues. But a restoration of computing system to point of prior troubleshooting may be required • Perform simple tests to ensure OS issues have been rectified • Update internal documents/records on problem report system and history log of the problematic computing system 3. Exhibit professionalism • Apply industry best practices when supporting operating systems • Follow organisation safety procedures when handling any hardware or equipment during the troubleshooting process
Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Gather sufficient information from user, problem report, internal records, etc. to gain a preliminary understanding of OS issues • Systematically plan and apply troubleshooting methodologies to reproduce and identify the cause of OS issues • Use diagnostic tools and system functions during the problem identification stage • To provide rectification to the OS issues and follow the organisation's procedures and guidelines for completing after event documents
Remark	

Title	Perform remote support
Code	107907L3
Description	This unit of competency applies to support personnel who are responsible for providing remote support. In a structure support team this would be a Level 2 support personnel where Level 2 is normally the first point of escalation, provides guidance and instructions to Level 1. Level2 is where the support personnel take ownership of incidents where subject matter expertise and experience is required for diagnosis. However, this UoC concerned only remote support competencies and does not distinguish the organization level.
Level	3
Credit	3

Competency	Performance Requirements
	1. Knowledge to perform remote support:
	
	- Possess good communication and interpersonal skills
	- Possess remote support skills capable of performing troubleshooting and providing systematic instructions for remote problem solving
	- Possess good knowledge and operating remote support applications
	- Understand committed Service Level Agreement (SLA) and standards
	- Possess good knowledge of problem escalation procedures and guidelines
	- Possess basic knowledge of the organisation computer hardware, Operating System (OS), applications and network equipment
	
	2. Performing remote support
	
	- Comprehend reported problem from Trouble Ticket system (TTS)/problem report system to understand symptoms and diagnostics from support desk colleague (level 1 support)
	- Search TTS/problem report system to determine if similar issues and/or solutions exist
	- Communicate with the customers/users to explain actions that will be performed to resolve the issue, such as:
	    o Need to collect more information related to the reported issue
	    o Need to remote access to user's system
	    o Will instruct the user to self-rectify the issue upon determination that the user is capable of self-rectification
	- If remote access/control is necessary, determine customer/user's comfort level to have remote access feature of the system turn on and installation of remote access software. To gain customer/user's support it is necessary to explain:
	    o How the remote access work compare with on-premise support
	    o There are no security risks
	    o Benefits of remote access/control
	- Perform troubleshoot and/or apply solution to correct the reported issue. If remote solution cannot fix the issue then offer to customer/user the on-premise support option
	- Confirm solution is acceptable with customer/user
	- Uninstall any application and/or reset configurations that were used for the remote support purpose and remind users to set off remote support functions on their system
	- Document all activities and record changed setting in the TTS/problem report. Where necessary, coordinate with other colleagues, such as requesting on-premise engineers to visit the customers/users
	
	3. Exhibit professionalism
	
	- Possess customer service oriented attitude
	- Always keep customer informed of actions and status of the rectification process

	• Follow industry best practices to use best remote support application to provide remote support
Assessment Criteria	The integrated outcome requirements of this UoC are the abilities to: • Comprehend the reported problem from the internal TTS/problem report system and able to update the appropriate record in accordance with the organisation's procedures after the completion of the remote support session • Persuade customers/users to allow remote access/control to their system for troubleshooting and/or correcting of issues • Perform the remote support to the satisfaction of customers/users
Remark	

Functional Area - System and Hardware Support

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	

Title	Perform simple web page update
Code	107908L2
Description	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:
	    o Add/remove text contents
	    o Correct broken links or references
	    o Insert new or delete old links or references
	    o 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

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	

Title	Troubleshoot web browser and connection issues
Code	107909L3
Description	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
	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:
	    o What are the types of issue user is experiencing,
	    o What type of browser
	    o 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:
	    o Verify the client is actually connected to the network (LAN or mobile)
	    o Verify client has acquired a valid IP and DNS address
	    o Verify correct proxy server setting
	    o 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	

Title	Maintain website performance
Code	107910L3
Description	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
	    o If loading is high, consider off load some of the tasks from the server
	    o 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:
	    o Minimise size of webpage
	    o Minimise the use of nested table
	    o Avoid using oversized image file straight from camera. Resize image files to a match the purpose
	    o 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	

Title	Build simple web site using content management systems
Code	107911L3
Description	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
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	

Title	Maintain website
Code	107912L3
Description	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
	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:
	    o Visitor feedbacks or user complaints
	    o Results of website testing tools
	    o Monitoring/log statistics
	    o Alerts of website outage
	• Periodically perform tests including but not limited to the following:
	    o Access to the website is still possible
	    o Web contents are compatible with different browsers and different clients (mobiles and desktops)
	    o No broken links
	    o Software are updated
	    o Access and download speed
	    o 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
	    o Pages entered on and exited on
	    o Time spent on the site
	    o Bounce rate
	    o Referring sites
	    o 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 (Version 2) 能力標準說明(第二版)					Specification of Competency Standards (Version 1) 能力標準說明(第一版)			
Specification of Competency Standards (SCS) 能力標準說明	Functional Area 職能範疇	UoC Code 能力單元編號	UoC Title	能力單元名稱	UoC Code 能力單元編號	UoC Title	能力單元名稱	Remarks
Communications and Information Services 通訊與訊息服務	Network Infrastructure and Operation 網絡基建及營運	111429L4	Implementing monitoring equipment to monitor infrastructure failure and security breaches	實施設備監控，以監控基建故障和安全性漏洞	ITCSNO431A	Implementing monitoring equipment to monitor infrastructure failure and security breaches	實施監控設備，以監控基建故障和安全性漏洞	Replacement of UoC 取代能力單元
		111430L4	Develop a plan to monitor network infrastructure performance	管理網絡基礎設施性能	108058L3 ITCSNO418A	Monitor performance of digital media infrastructure Analysing performance reports	監控數碼媒體基建性能 分析效能報告	Replacement of UoC 取代能力單元
		111106L3	Perform installation, configuration and testing of network equipment and devices	進行網絡設備的安裝，配置和測試	ITCSNO306A	Perform installation, configuration and testing of network equipment	進行網絡設備的安裝，配置和測試	Replacement of UoC 取代能力單元
		111107L4	Perform network testing	進行網絡測試	ITCSNO424A	Perform network testing	進行網絡測試	Replacement of UoC 取代能力單元
Digital Media Technology 數碼媒體科技	DMT Architecture 數碼媒體科技架構	111108L6	Develop digital content delivery network strategy	開發數碼內容傳遞網絡策略	108052L6	Develop content delivery network strategy for digital media business	為數碼媒體業務開發內容傳遞網絡策略	Replacement of UoC 取代能力單元
	Marketing Management 營銷管理	111109L7	Formulate digital marketing strategy	制定數碼營銷策略	107914L7	Formulate digital marketing strategy	制定數碼營銷策略	Replacement of UoC 取代能力單元
		111110L6	Formulate digital marketing strategy for Mainland China	制定在中國內地使用的數碼營銷策略	108027L6	Formulate digital marketing strategy for Mainland China	制定在中國內地使用的數碼營銷策略	Replacement of UoC 取代能力單元
	Operational Management 營運管理	111115L4	Create motion graphics	創作動態圖形	107944L4	Create motion graphics	創作動態圖形	Replacement of UoC 取代能力單元
		111119L3	Prepare for live video and audio capture	準備實時視頻和音頻擷取	107970L3	Prepare for digital video capture	準備數碼視訊擷取	Replacement of UoC 取代能力單元
Operation and Support 營運與支援	System & Hardware 系統與硬件支援	111122L2	Record problem/fault reports	記錄問題/錯誤報告	ITCSNO207A	Record problem/fault reports	記錄問題/錯誤報告	Replacement of UoC 取代能力單元
Software Products and Software Services 軟件產品及軟件服務	Architecture 軟件架構	111123L6	Define data governance policies and architecture principles	訂定資料管理政策和架構原則	ITSWAR608A	Define data manage policies and architecture principles	訂定資料管理政策和架構原則	Replacement of UoC 取代能力單元
		111124L6	Develop application integration architecture	發展應用系統綜合架構模式	ITSWAR617A ITSWAR618A	Recommend application integration architecture models Develop application integration architecture resources	推薦應用系統綜合架構模式 發展應用系統綜合架構模式的資源	Replacement of UoC 取代能力單元

Specification of Competency Standards (SCS) 能力標準說明	Functional Area 職能範疇	Specification of Competency Standards (Version 2) 能力標準說明(第二版)			Specification of Competency Standards (Version 1) 能力標準說明(第一版)			Remarks 備註
		UoC Code 能力單元編號	UoC Title	能力單元名稱	UoC Code 能力單元編號	UoC Title	能力單元名稱	
Software Products and Software Services 軟件產品及軟件服務	Architecture 軟件架構	111125L6	Review, design and re-engineer business processes to form a new business architecture	檢討、設計及重整業務程序以建立新的商業架構	ITSWAR607A	Review, design and re-engineer business processes to form a new business architecture	檢討、設計及重整業務程序以建立新的商業架構	Replacement of UoC 取代能力單元
		111126L6	Determine technology mix for the design and development of embedded software systems	確定嵌入式軟件系統的設計和發展的技術組合	ITSWAR620A	Determine technology mix for the design and development of embedded software systems	確定嵌入式軟件系統的設計和發展的技術組合	Replacement of UoC 取代能力單元
		111127L5	Define metrics to ensure that a technology architecture meets the business goals	訂定度量指標，確保技術架構符合企業目標	ITSWAR508A	Define metrics to ensure that a technology architecture meets the business goals	訂定度量指標，確保技術架構符合企業目標	Replacement of UoC 取代能力單元
		111129L5	Model technology architecture	塑造技術架構	ITSWAR507A	Model technology architecture	塑造技術架構	Replacement of UoC 取代能力單元
	Data Science 數據科學	111138L6	Define and establish the data architectures	訂定和建立資料架構	ITSWAR610A	Define and establish a data architectures	訂定和建立資料架構	Replacement of UoC 取代能力單元
		111139L6	Check usability of a target data architecture	檢查目標資料架構的實用性	ITSWAR612A	Check usability of a target data architecture	檢查目標資料架構的實用性	Replacement of UoC 取代能力單元
	Design, Development & Maintenance 設計、開發與維護	111155L6	Define a system migration plan	訂定系統遷移計劃	ITSWDM611A	Define a software deployment / migration plan	訂定軟件部署/遷移計劃	Replacement of UoC 取代能力單元
		111157L6	Perform risk assessment on system migration	執行系統遷移的風險評估	ITSWDM610A	Perform risk assessment on software deployment and migration	執行軟件部署和遷移的風險評估	Replacement of UoC 取代能力單元
		111159L4	Verify and validate that the deployed / migrated software and the existing software are functioning properly	核實和確認部署/遷移的軟件和現有的軟件的正常運作	ITSWDM405A	Verify and validate that the deployed/migrated software and the existing software are functioning properly in the context of deploying and migrating software	核實和確認部署/遷移的軟件和現有的軟件的正常運作	Replacement of UoC 取代能力單元
		111160L4	Perform system testing against user, technical and hosting requirements	針對用戶、技術和託管要求執行系統測試	ITSWDM401A	Perform testing activities to facilitate different levels of testing	執行測試活動，促進不同程度的測試	Replacement of UoC 取代能力單元
	Generic Skills 通用技能	111161L5	Acquire and protect the copyrights and IP rights related to IT	獲取和保修與資訊科技有關的版權和知識產權	ITSWGS523A	Acquire and protect the copyrights and IP rights related to IT	獲取和保修與資訊科技有關的版權和知識產權	Replacement of UoC 取代能力單元

Specification of Competency Standards (Version 2) 能力標準說明(第二版)					Specification of Competency Standards (Version 1) 能力標準說明(第一版)			
Specification of Competency Standards (SCS) 能力標準說明	Functional Area 職能範疇	UoC Code 能力單元編號	UoC Title	能力單元名稱	UoC Code 能力單元編號	UoC Title	能力單元名稱	Remarks
Software Products and Software Services 軟件產品及軟件服務	Information Security 資訊保安	111164L6	Develop information security standard, policies and guidelines for the organization	為企業制訂網絡安全標準、政策和準則	ITCSPL606A	Establish security policy for the products / services	為產品/服務建立保密政策	Replacement of UoC 取代能力單元
	Information Security 資訊保安	111165L6	Develop response and recovery plans	制訂應變和復原計劃	ITSWIS614A	Develop response and recovery plans	制訂應變和復原計劃	Replacement of UoC 取代能力單元
		111166L6	Review key controls metrics regularly to fulfill the security standard	定期檢討關鍵績效指標以達到保安標準	ITSWIS609A	Establish metrics to manage information security governance framework	設立處理資訊保安管治架構的度量指標	Replacement of UoC 取代能力單元
		111170L5	Develop procedures to implement incident response plan	制定程序以實施事件應對計劃	ITSWIS614A	Develop response and recovery plans	制訂應變和復原計劃	Replacement of UoC 取代能力單元
		111171L5	Develop procedures to maintain and comply with the information security standard and policies of the organisation	制定程序以維護和遵守企業的網絡安全標準和政策	ITSWIS506A	Develop information security practices and procedures	制訂資訊保安慣例和常規	Replacement of UoC 取代能力單元
		111174L5	Identify the potential security threats to the organisation	確定和評估企業的潛在保安風險	ITSWIS605A	Identify the potential security threats to the company	確定和評估風險	Replacement of UoC 取代能力單元
		111175L5	Manage the execution of response and recovery plans	處理應變和復原計劃的執行	ITSWIS511A	Manage the execution of response and recovery plans	處理應變和復原計劃的執行	Replacement of UoC 取代能力單元
		111176L5	Perform network security assessment for the organization	為企業進行網絡安全評估	ITCSNO530A	Define network infrastructure access policies	釐定網絡基建的接入政策	Replacement of UoC 取代能力單元
		111177L5	Prepare and deliver information system security audit report	準備和提交資訊系統保安審計報告	ITSWIS514A	Prepare and deliver information system security audit report	準備和提交資訊系統保安審計報告	Replacement of UoC 取代能力單元
		111178L5	Prepare documentation to report the security testing and findings	準備安全測試和結果報告	ITSWIS512A	Establish procedures documenting security incident	建立記錄保安事件的程序	Replacement of UoC 取代能力單元
		111179L5	Propose appropriate countermeasures to prevent security attacks	提出適當的對策以防止安全攻擊	ITSWIS525A	Minimize information security risks	減低資訊保安風險	Replacement of UoC 取代能力單元

Specification of Competency Standards (Version 2) 能力標準說明(第二版)					Specification of Competency Standards (Version 1) 能力標準說明(第一版)			
Specification of Competency Standards (SCS) 能力標準說明	Functional Area 職能範疇	UoC Code 能力單元編號	UoC Title	能力單元名稱	UoC Code 能力單元編號	UoC Title	能力單元名稱	Remarks
Software Products and Software Services 軟件產品及軟件服務	Project Management 項目管理	111197L5	Conduct solicitation planning	實施徵集計劃	ITSWPM521A	Conduct solicitation planning	實施徵集計劃	Replacement of UoC 取代能力單元
		111198L5	Conduct project closure with respect to time	處理與時間有關的項目結束	ITSWPM505A	Conduct project closure with respect to time	處理與時間有關的項目結束	Replacement of UoC 取代能力單元
	Project Management 項目管理	111199L4	Analyze the available solutions from IT service providers	分析資訊科技服務提供商的解決方案	ITSWPM523A	Conduct source selection and/or contract development	進行外發的來源挑選和/或合同發展	Replacement of UoC 取代能力單元
		111200L4	Prepare system operation documentation	編制系統操作文檔	ITSWPM403A	Establish project communications documentation requirements	制定項目通訊的檔案編制要求	Replacement of UoC 取代能力單元
	Strategic Management 策略管理	111201L6	Formulate business strategies and policies	制定業務策略及政策	ITSWSM602A	Formulate business strategies and policies	制定業務策略及政策	Replacement of UoC 取代能力單元
		111202L6	Identify and evaluate information technologies that support the objectives of an organisation	辨識及評估支援企業的目標的資訊科技	ITSWSM612A	Identify and evaluate information technologies that support the objectives of an organisation	辨識及評估支援組織的目標的資訊科技	Replacement of UoC 取代能力單元
		111203L6	Maintain the portfolio management with different stakeholders	維護與不同持份者的投資組合管理	ITSWGS618A	Manage and maintain the portfolio and relationship with business partners	處理和保持與商務夥伴的投資組合和關係	Replacement of UoC 取代能力單元
		111205L6	Review and comply with organisational policies and procedures, relevant laws and regulatory requirements	檢討及遵從企業的政策和程序、相關法律和監管要求	ITSWGS624A ITSWGS602A	Comply with relevant laws and regulatory requirements Comply with organisational policies and procedures, relevant laws and regulatory requirements	遵照有關的法律和管理要求 遵從機構的政策和程序、相關法律和監管要求	Replacement of UoC 取代能力單元
		111206L6	Set policy to control data security and privacy	制定政策管理資料保安及私隱	ITSWSM611A	Set policy to control data security and privacy	制定政策管理資料保安及私隱	Replacement of UoC 取代能力單元
		111209L5	Establish a business continuity planning strategy	建立商業延續計劃的策略	ITSWIS519A	Establish a business continuity planning strategy	建立商業延續計劃的策略	Replacement of UoC 取代能力單元
		111210L5	Formulate IT plan	擬定資訊科技計劃	ITSWSM503A	Formulate IT plan	擬定資訊科技計劃	Replacement of UoC 取代能力單元

		Specification of Competency Standards (Version 2) 能力標準說明(第二版)				Specification of Competency Standards (Version 1) 能力標準說明(第一版)			
Specification of Competency Standards (SCS) 能力標準說明	Functional Area 職能範疇	UoC Code 能力單元編號	UoC Title	能力單元名稱	UoC Code 能力單元編號	UoC Title	能力單元名稱	Remarks
Software Products and Software Services 軟件產品及軟件服務	Strategic Management 策略管理	111212L6	Formulate global and local business strategies	制定全球和本地的業務策略	108015L7 ITCSSG503A ITCSSG602A	Formulate global and local business strategy Formulate global and local marketing strategies Define business strategies and policies	制定全球和本地的業務策略 制定全球及地區市場策略 釐定業務策略和政策	Replacement of UoC 取代能力單元
		111213L6	Formulate strategies on business relation management	制定業務關係管理策略	ITSWGS618A ITCSSG508A ITCSSG521A	Manage and maintain the portfolio and relationship with business partners Formulate partner/supplier relationship strategies Manage and maintain the portfolio and relationship with business partners	處理和保持與商務夥伴的投資組合和關係 制定合作夥伴/供應商關係之策略 管理和維繫與業務合作夥伴之間的關係和組合	Replacement of UoC 取代能力單元
		111214L6	Formulate human resource strategy	制定人力資源策略	108021L5 ITCSSG606A	Formulate human resource strategy Formulate human resource strategies	制定人力資源策略 制定人力資源策略	Replacement of UoC 取代能力單元
		111215L6	Formulate vision and mission statements	制定願景和使命聲明	ITSWSM601A ITCSSG601A	Formulate vision and mission statements Formulate vision and mission statements	制定遠景及使命聲明 制定願景和使命的聲明	Replacement of UoC 取代能力單元
		111216L6	Establish and implement information management and control policy	建立和實施資訊管理和保安政策	ITSWSM611A ITSWSM506A 108022L5	Set policy to control data security and privacy Collect and distribute disseminate information Manage information strategy to facilitate product development and marketing	制定政策管理資料保安及私隱 搜集及分發資訊 管理資訊策略以促進產品開發和市場營銷	Replacement of UoC 取代能力單元
		111217L5	Manage marketing and public relation plans	管理營銷和公關計劃	ITSWSM508A ITCSSG403A	Manage product/services brand through the use of IT Implement Public Relation Plans	利用資訊科技管理產品/服務品牌 實施公關計劃	Replacement of UoC 取代能力單元
		111218L5	Establish contingency and risk mitigation plans	建立應急和風險緩解策略	ITSWGS609A ITCSSG501A ITCSSG512A	Develop business continuity plans and disaster recovery plans related to IT Formulate risk mitigation strategies and plans Develop business continuity and disaster recovery plans	確定和評估與資訊科技有關的風險因素 制定風險緩解策略和計劃 發展業務連續性和災難恢復計劃	Replacement of UoC 取代能力單元