Supporting holistic delivery: developing learning activities to integrate core and occupational specialism content

T Level in Digital Support Services
    Core component: 03 Data
    Occupational specialism: Digital infrastructure
ETFOUNDATION.CO.UK

Course:	**T Level in Digital Support Services** Digital Support Services (qualhub.co.uk)
Component:	**Core component: 03 Data** **Occupational specialism: Digital infrastructure**
Related components and performance outcomes:	**Core component** • **R3.1** The fundamental characteristics of data • **R3.4** The concepts involved in data entry and maintenance • **R3.8** Types of data access management across platforms in a digital environment • **R3.9** Types and application of access control methods **Occupational specialism: Digital infrastructure** **PO1:** Apply procedures and controls to maintain the digital security of an organisation and its data • **K1.23** The purpose and application of legislation, industry standards and regulatory compliance and industry best practice guidelines for the security of information systems within digital infrastructure • **K1.25** Methods of managing and controlling access to digital systems and their application in the design of network security architecture **PO2:** Explain, install, configure, test and manage both physical and virtual infrastructure • **K2.3** The elements of infrastructure and associated technologies • **K2.7** The advantages and limitations of self-hosted and cloud-hosted virtual servers • **K2.12** The considerations involved in setting up a simple VPN to enable secure remote access **Skills development in Occupational specialism: Digital infrastructure pathway**

		• **S1.1** Apply and maintain procedures and security controls in the installation, configuration and support of physical and virtual infrastructure to ensure confidentiality, integrity and availability • **S1.3** Explain the importance of organisational and departmental policies and procedures in respect of adherence to security • **S1.5** Conduct a security risk assessment in line with the risk management process for a system (for example, a device connected to a local area network or LAN) • **S1.6** Demonstrate continuous improvement through the application of risk mitigation in maintaining the digital security of an organisation and its data in a digital infrastructure context • **S2.1** Explain the fundamentals of network infrastructure **Employer-set project (core component): Digital infrastructure** • A01, A02 and A03

Session	Learning outcome(s)	Learning activities	Resources	Assessment
1	**Core knowledge and skills** **R3.1** The fundamental characteristics of data: • storing data • cloud storage. **Occupational specialism: Digital infrastructure pathway**	**Starter activity** Quiz on data storage. **Tutor-led** Explain in general what data storages are. **Learner activity 1** Learners will be divided into small groups and discuss the following data	Quiz questions and answers on Session 1 - Quiz.pptx PowerPoint Session 1.pptx Flipcharts and marker pen for group discussion	Assessment of prior knowledge on data storage Tutor questioning to check for understanding during delivery

		storages with answers to be written on the flipchart:	Computers with internet access for research	Self-assessment of responses to questions
	PO2: Explain, install, configure, test and manage both physical and virtual infrastructure • **K2.3** The elements of infrastructure and associated technologies • **K2.7** The advantages and limitations of self-hosted and cloud-hosted virtual servers **Skills development in Occupational specialism: Digital infrastructure pathway** • **S1.5** Conduct a security risk assessment in line with the risk management process for a system (for example, a device connected to a local area network or LAN)	• SSD (solid state drive) • HDD (hard disk drive) • File servers • NAS (Network-attached storage) • SAN (storage area network). For each of the above, learners must discuss the following: • explain why a computer system needs secondary storage • state the different types of physical/on-premises storage and describe their functional characteristics • compare and contrast. Each group to present their answers to the class. Each group to take note on anything they have missed in their discussion. **Tutor-led** Introduction to elements of infrastructure and technologies: tutor to lead an introduction and discussion exploring network devices, end user devices and storage solutions. **Learner activity 2**	Microsoft Office applications	Learners work in groups to share their responses

| | | Working in groups, learners to create a presentation on one of the following topics and feed back to the class:
• identify a range of network devices
• identify a range of end user devices
• identify a range of storage devices.

Tutor-led
Tutor to introduce and discuss examples of various types of cloud storage.

Learner activity 3
Learners to research and discuss in pairs the following cloud storages and include advantages and disadvantages for each one:
• file storage
• object storage
• block storage
• elastic/scalable cloud
• cloud-based databases.

Tutor-led
Tutor to introduce learners to servers with a comparison of physical versus virtual versus cloud-hosted, with considerations of the advantages and disadvantages of each one.

Learner activity 4
Learners to work independently to research costings for cloud-hosted | | |

		servers and a case study comparing cloud with physical. **Skills development activity** Research and apply the risk management process, which includes the following: • identify possible risks in the system • calculate the probability and impact of the identified risk • analyse and prioritise based on level of risk to system.		

2	**<u>Core knowledge and skills</u>**
	R3.4 The concepts involved in data entry and maintenance
	• Data entry:
	  • reducing risk of data entry errors (validation and verification)
	  • privacy (compliance with standards and legislation for usage and storage).
		Tutor-led:
		Tutor will explain the concepts involved in data entry and maintenance.
		
		Learner activity 1
		Data entry task: learners to be given a timed data entry task. An example of an appropriate task would be the requirement to manually enter values into a spreadsheet. This should last no longer than 15 minutes.
		
		Following completion of the activity, the tutor will discuss the answers with the class.
		
		Tutor-led
		Tutor to introduce the concepts involved in data entry, relating this to the learners'
			PowerPoint Session 2.pptx
			
			Session 2 Activity 1 - Student version.docx
			
			Session 2 Activity 1 - Tutor version.docx
			
			Flipcharts and marker pen for group discussion
			
			Computers with internet access for research
			
			Microsoft Office applications
				Assessment of prior knowledge
				
				Tutor questioning to check for understanding during delivery
				
				Self-assessment of responses to questions
				
				Learners work in groups to share their responses

Occupational specialism: Digital infrastructure pathway PO1: Apply procedures and controls to maintain the digital security of an organisation and its data • **K1.23** The purpose and application of legislation, industry standards and regulatory compliance and industry best practice guidelines for the security of information systems within digital infrastructure **Skills development in Occupational specialism: Digital infrastructure pathway** • **S1.6** Demonstrate continuous improvement through the application of risk mitigation in maintaining the	experiences with the previous data entry task. **Learner activity 2** Learners to find a website that includes a data entry screen – for example, a retail website. Investigate the validation techniques that have been used and the error messages shown when a data entry error has been made. On completion, learners will discuss in group how using validation techniques and error messages will decrease the impact of data entry errors on the website's owner, taking into consideration the following: • data type/type of data to be entered • risk of errors • legal issues • maintenance and integrity of data • resource considerations. **Skills development activity** Research and apply risk mitigation techniques to the identified threats, vulnerabilities or incidents detected in end user devices – for example, installing remote monitoring and management (RMM) software, device hardening.	

	digital security of an organisation and its data in a digital infrastructure context	**Tutor-led** Tutor to lead an introduction and discussion on legislation, standards and compliance: • EU General Data Protection Regulation (GDPR) • Computer Misuse Act 1990 • ISO 27001:2017 • Payment Card Industry Data Security Standard (PCI DSS) • National Cyber Security Centre (NCSC) '10 Steps to Cyber Security' • Open Web Application Security Project (OWASP). **Learner activity 3** Working in groups, each group is assigned one of the topics above to create a leaflet providing guidance for a digital business.		
3	**Core knowledge and skills** **R3.8** Types of data access management across platforms in a digital environment: • user access controls	**Tutor-led** Introduction to access controls and APIs. Tutor-led discussion and presentation on access control. This should include the following: • physical access • remote access • permissions • authentication.	PowerPoint Session 3.pptx Flipcharts and marker pen for group discussion Computers with internet access for research	Assessment of prior knowledge Tutor questioning to check for understanding during delivery

		Learner activity 1	Microsoft Office applications	Self-assessment of responses to questions
	• application programming interface (API). **Occupational specialism: Digital infrastructure pathway** PO2: Explain, install, configure, test and manage both physical and virtual infrastructure • **K2.12** The considerations involved in setting up a simple VPN to enable secure remote access **Skills development in Occupational specialism: Digital infrastructure pathway** • **S2.1** Explain the fundamentals of network infrastructure	Design a server room: learners to be given the requirements for a server room for an organisation. They must then design the security measures that will be implemented from an access control perspective. This should be designed visually and can be fed back to the class. **Tutor-led** Learners to be introduced to the concept of APIs and how they allow information access. **Learner activity 2** Learners to research APIs that would be beneficial in their future job role. **Tutor-led** Introduction to servers: tutor to introduce learners to the concepts of virtualisation and secure remote access. Tutor to explore the concept of virtualisation and areas of application: • VPN (virtual private network) • RDP (remote desktop protocol) • LOM (lights-out management) • SSH (secure shell). **Learner activity 3**		Learners work in groups to share their responses

		Learners split into four groups and each group to create a presentation for the four different remote access methods. This should explore advantages, disadvantages, configurations (both server and client, if required) and security. **Skills development activity** Identify and explain the purpose and application of network infrastructure.		
4	**Core knowledge and skills** **R3.9** Types and application of access control methods **Occupational specialism: Digital infrastructure pathway** PO1: Apply procedures and controls to maintain the digital security of an organisation and its data • **K1.25** Methods of managing and controlling access to digital systems and their application	**Tutor-led** Introduction to access control methods: tutor-led discussion and presentation on types of control. • RBAC (role-based access control) • ABAC (attribute-based access control) • MAC (mandatory access control) • DAC (discretionary access control). **Learner activity 1** Access control activity: learners to be given a list of multiple answer questions. Class discussion to support. **Skills development activity**	PowerPoint Session 4.pptx Session 4 Activity 1 - Student version.docx Flipcharts and marker pen for group discussion Computers with internet access for research Microsoft Office applications	Assessment of prior knowledge Tutor questioning to check for understanding during delivery Self-assessment of responses to questions Learners work in groups to share their responses

		in the design of network security architecture	Configure and apply appropriate access control methods to physical or virtual networks.		
		Skills development in Occupational specialism: Digital infrastructure pathway • **S1.1** Apply and maintain procedures and security controls in the installation, configuration and support of physical and virtual infrastructure to ensure confidentiality, integrity and availability • **S1.3** Explain the importance of organisational and departmental policies and procedures in respect of adherence to security	**Learner activity 2** Learners to work in groups to create a presentation on the following. Each topic must be covered, so group sizes will vary. The presentation will be delivered to the class. • Managing and controlling access to systems. • Physical and virtual methods of managing and securing network traffic. • Techniques applied to ensure cybersecurity for internet connected devices. • Importance of cybersecurity to organisations and society. • The fundamentals of network topologies. • The application of cybersecurity principles. **Tutor-led** Tutor-led discussion on common vulnerabilities. **Learner activity 3**		

	Employer-set project (core component): Digital infrastructure • A01, A02 and A03	In small groups, learners to discuss each of the following and their impact, including any security controls: • missing patches, firmware and security updates • password vulnerabilities • insecure BIOS/UEFI • misconfigurations • lack of protection software • disposal of data/devices • inadequate back-up process • DHCP spoofing • VLAN attacks • misconfigured firewalls or ACLs • exposed services or ports. **Skills development activity** Explain the potential impact on security if policies and procedures are not adhered to – for example, danger to life or privacy. **Employer-set project: project brief** • A01: Plan their approach to meeting the project brief • A02: Apply core knowledge and skills, as appropriate, to infrastructure support and maintenance • A03: Select relevant techniques and resources to meet the brief		