

**Unit 503 Install, Configure and Integrate Networked Hardware and Software
Level 3 (Core)**

Rationale

This unit will enable the candidate to install, integrate and configure ICT components and networks.

There are 5 outcomes to this unit. The candidate will be able to:

1. carry out risk assessment and ensure health and safety procedures are followed
2. survey the user environment for installation of hardware equipment and systems
3. install hardware equipment and systems
4. install and configure systems software
5. expand (by integration) ICT systems to allow additional facilities.

Guided learning hours

The recommended guided learning hours for this unit are 90 hours.

Connections with other awards

NVQ links

Outcome	This award contributes to the knowledge and understanding of the following elements of NVQ(s)
	<i>C&G 4300 Installing and Supporting IT Systems Level 3</i>
1	206.1 Identify the hazards and evaluate the risks in your workplace
1	206.2 Reduce the risks to Health and Safety in your workplace
2, 5	314.1 Prepare for the installation of hardware products
2, 3	314.2 Make hardware products ready for installation
2, 3	314.3 Assemble hardware products
3	314.4 Load and use software associated with hardware products
3, 4	314.5 Complete the installation of hardware products
2, 4	315.1 Prepare for the installation of software
4	315.2 Load and configure software
4	315.3 Complete the installation of software
3, 4, 5	316.1 Plan for system testing
3, 4, 5	316.2 Carry out system testing
3, 4, 5	316.3 Examine and respond to the results of system tests
	<i>C&G 4348 IT Services (Customer Systems Support) Level 3</i>
3, 4, 5	21.1 Prepare tests for IT systems
3, 4, 5	21.2 Test IT systems
4, 5	21.3 Return IT systems to operation after testing
1, 5	30.1 Survey the customer environment for the installation of hardware systems
3, 5	30.2 Install hardware systems
4, 5	30.3 Commission hardware systems for operation
1, 5	31.1 Survey the customer environment for the installation of software systems
3, 4	31.2 Install software systems
4, 5	31.3 Commission software systems for operation
5	32.1 Identify methods to integrate IT systems
5	32.2 Integrate IT systems

Key Skills links

Communication	C3
Application of number	
IT	IT 2
Working with others	
Improving own learning	LP 2
Problem solving	PS 3

Assessment

Assessment will be by means of a **set assignment** covering practical activities, and a **multiple choice test** covering underpinning knowledge.

Outcome 1: Carry out risk assessment and ensure Health and Safety procedures are followed

	Candidate's signature	Date
<p>Practical activities The candidate will be able to:</p> <ol style="list-style-type: none"> 1. carry out a risk assessment of the work area 2. maintain Health and Safety records and documentation 3. identify accurately any conflicts which exist between the working environment and statutory requirements 4. make recommendations for changes to procedures and policies in the working environment. 		
<p>Underpinning knowledge The candidate will be able to:</p> <ol style="list-style-type: none"> 1. describe employers and employees duties as required by relevant Health and Safety legislation 2. explain the reasons for keeping Health and Safety records 3. describe effective methods for monitoring activities and understanding of others in Health and Safety 4. explain why it is important that people have up to date information about applicable Health and Safety procedures, and understand their responsibilities 5. describe effective methods of communicating Health and Safety procedures, e.g. <ul style="list-style-type: none"> • oral • written • electronic 6. describe how risks may result from the following hazards, e.g. <ul style="list-style-type: none"> • the use of hazardous substances • the use and maintenance of plant, equipment and materials • poor working practices • unsafe behaviour • accidental breakage and spillage • obstructions • personal health 7. describe how hazards are categorised as low or high risk 8. explain the benefits of risk assessment 9. explain the reasons why conflicts that exist between the working practices and statutory requirements need to be reported promptly and accurately 10. describe the importance of reporting 'near misses' and initiating corrective action. 		

Outcome 2: Survey the user environment for installation of hardware equipment and systems

	Candidate's signature	Date
<p>Practical activities The candidate will be able to:</p> <ol style="list-style-type: none"> 1. prepare a site survey checklist for the installation of hardware equipment/systems, e.g. <ul style="list-style-type: none"> • identify factors which might affect installation • identify potential problems 2. plan access to the user's environment 3. survey the user's environment for, e.g. <ul style="list-style-type: none"> • positioning of network cabling (or need for wireless systems), hubs, routers • location of stand alone equipment • location of client servers • connection of modem to telephone lines • access to power supply 4. prepare and deliver a report on the survey 5. create an installation plan and schedule. 		
<p>Underpinning knowledge The candidate will be able to:</p> <ol style="list-style-type: none"> 1. describe the reasons for surveying the user's environment prior to the installation of hardware equipment/systems, e.g. <ul style="list-style-type: none"> • safety • suitability • minimise disruption 2. describe factors to be considered prior to installing hardware equipment and systems <ul style="list-style-type: none"> • access constraints- security, physical access, operational disruption • environmental – existing equipment, availability of utilities and services, ambient conditions 3. identify potential problems which might affect installation, e.g. <ul style="list-style-type: none"> • health and safety issues • accommodation • availability of utilities and services • access to building • structure for cabling 4. state reasons for not proceeding with installation, e.g. health and safety issues, availability of utilities and services 5. describe main points that should be included in an installation plan covering hardware equipment, system software and configuration. 		

Outcome 3: Install hardware equipment and systems

	Candidate's signature	Date
<p>Practical activities The candidate will be able to:</p> <ol style="list-style-type: none"> 1. install and test hardware and systems, e.g. <ul style="list-style-type: none"> • stand alone • peer to peer network • client server • network cabling, switches and routers • network interface cards (NIC) • workstation • network printer • modem (dial up, ADSL) 2. test equipment installed, to confirm successful installation 3. identify, investigate and resolve any problems encountered 4. maintain installation records. 		
<p>Underpinning knowledge The candidate will be able to:</p> <ol style="list-style-type: none"> 1. describe test procedures for different types of hardware equipment and systems, e.g. self test, diagnostics, manual tests 2. explain handling and transport procedures for hardware e.g. packaging, anti-static precautions, movement 3. describe types of network, e.g. <ul style="list-style-type: none"> • peer to peer • server based 4. identify network topologies, e.g. <ul style="list-style-type: none"> • ring • star • bus 5. describe the purpose of a network interface card (NIC) 6. identify suitable network cabling, e.g. <ul style="list-style-type: none"> • twisted pair • co-axial • fibre optic • wireless 7. describe the importance of keeping accurate installation records. 		

Outcome 4: Install and configure systems software

	Candidate's signature	Date
<p>Practical activities The candidate will be able to:</p> <ol style="list-style-type: none"> 1. check the integrity of the software to be installed, e.g. virus check, and the installation media, e.g. disk scan 2. install software <ul style="list-style-type: none"> • operating system/networked operating system • device drivers • applications, e.g. browser word processing, data base 3. set up and configure network, e.g. <ul style="list-style-type: none"> • user accounts • shared folders/access • user rights • group rights/permissions • passwords 4. configure maintenance routines, e.g. <ul style="list-style-type: none"> • system monitor • system tune up • back up routines • virus monitoring • firewalls • passwords • encryption • access policies 5. identify and investigate any problems encountered, resolve and record the detail 6. maintain installation records. 		
<p>Underpinning knowledge The candidate will be able to:</p> <ol style="list-style-type: none"> 1. describe the types of actions required to preserve the integrity of the existing system and data, e.g. backing up software and data, logging out users 2. explain why it is important to check the integrity of installation media e.g. completeness, free from corruption, virus free 3. identify potential conflicts between planned installation and user requirements, e.g. human, physical, technical, software levels 4. describe what type of tests can be applied to confirm successful installation of system software, e.g. built in diagnostics run, system loads successfully 5. explain what types of information should be recorded on installation records, e.g. name and version, licence number, contact/help numbers <p>Continued....</p>		

6. describe the importance of keeping accurate installation records
7. describe security arrangements, e.g.
 - confidentiality
 - copyright
 - data protection
 - data loss and back up
 - virus checking
 - firewalls.

Outcome 5: Expand (by integration) ICT systems to allow additional facilities

	Candidate's signature	Date
<p>Practical activities The candidate will be able to:</p> <ol style="list-style-type: none"> 1. determine the expected functionality and performance of the expanded ICT system, e.g. <ul style="list-style-type: none"> • additional workstation • additional printer • additional scanner 2. identify a suitable method for integrating the ICT system, e.g. <ul style="list-style-type: none"> • connection to an existing connecting point • creating additional connection points 3. check the additional components for compatibility with existing system 4. determine suitable configuration options for the intended additional components, e.g. <ul style="list-style-type: none"> • TCP/IP address • access authorisation • passwords • designations 5. determine what actions are required to preserve the integrity of any existing system or data, e.g. <ul style="list-style-type: none"> • back up • anti virus check • reconfiguration of firewall • re-organise user groups 6. prepare a plan for the integration of the ICT system which covers, e.g. <ul style="list-style-type: none"> • actions required to preserve the integrity of any existing system or data • configuration of components • installation of new components • tests to ensure that the expected functionality and performance have been achieved 7. install additional components and configure the systems 8. test the system to confirm that it functions 9. demonstrate integrated system and train users as necessary. 		

Underpinning knowledge

The candidate will be able to:

1. state circumstances in which components might be added to an existing system, e.g. new users, more capacity required, more/different output devices required, new functionality
2. state circumstances when components may be removed, e.g. obsolescence, over capacity, change of system requirements
3. identify causes of problems that can arise during expansion (integration) of ICT systems covering, e.g.
 - hardware incompatibility, e.g. revision level
 - software incompatibility, e.g. version level
4. describe the effects of problems that can arise during expansion (integration) of ICT systems
 - reduction in system performance
 - reduction in system function
 - reduction in system capacity
 - data loss or corruption
5. describe how ICT components can be configured to resolve problems covering:
 - physical configuration of hardware
 - logical configuration of hardware
 - configuration of software associated with hardware (e.g. drivers)
 - configuration of system software
 - configuration of application software
6. describe how to assess the function and performance required of the expanded (integrated) system
7. describe how to assess the additional components for compatibility with existing systems
8. describe the types of action required to preserve the integrity of the existing system and data, e.g. backing up software and data, logging out users
9. describe typical format and content of an expansion (integration) plan, e.g.
 - performance of existing systems
 - expected performance after expansion (integration)
 - actions to preserve the integrity of existing data and software
 - method of installation of new components (connection, configuration)
 - revised system configuration
 - testing method and expected results
 - user training requirements.