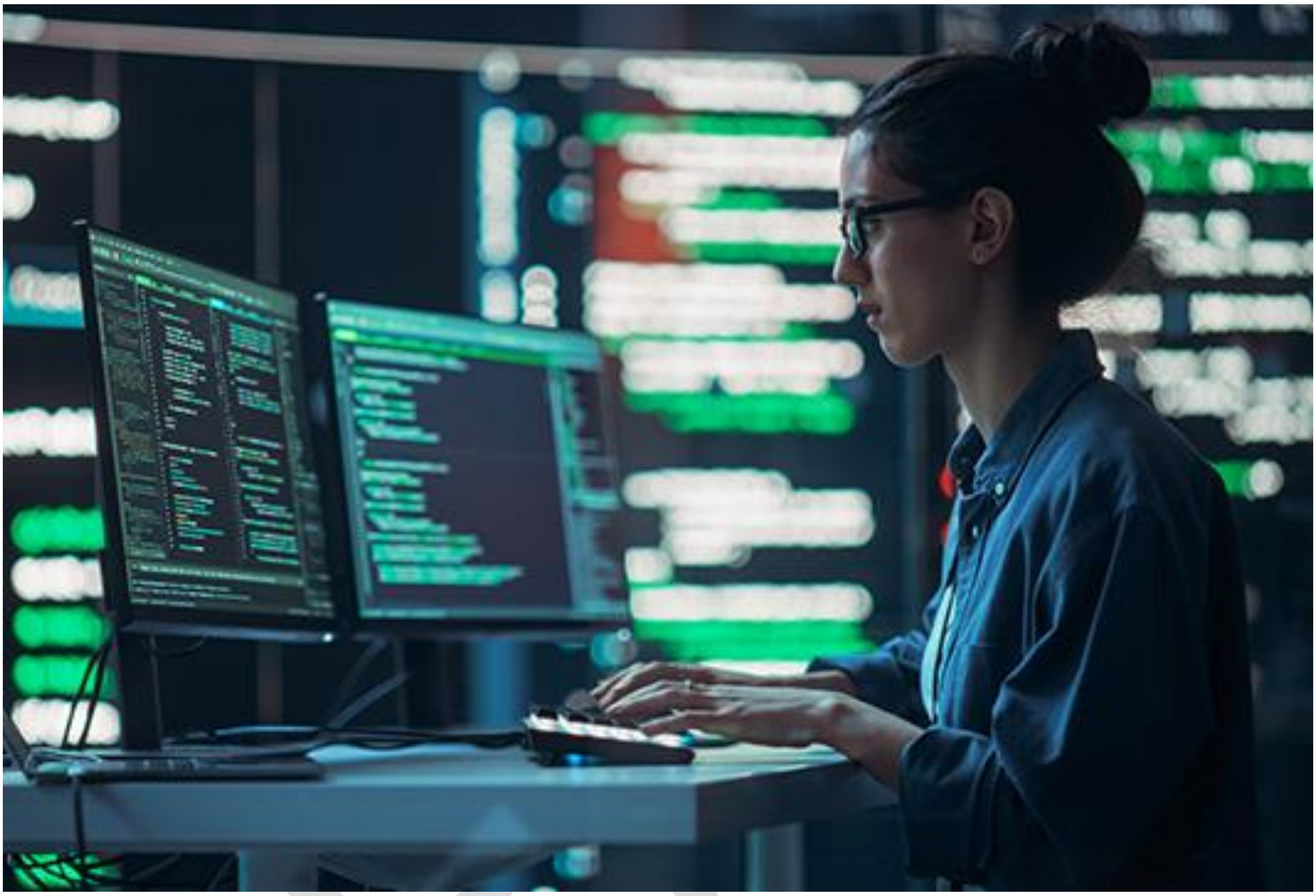
NCFE Level 3 Technical Occupational Entry in Cyber Security (Diploma)
QN: 610/4004/6



Qualification Specification

Version 1.0 August 2025

Visit ncfe.org.uk **Call** 0191 239 8000

Qualification summary

Qualification title	**NCFE Level 3 Technical Occupational Entry in Cyber Security (Diploma)**
Ofqual qualification number (QN)	610/4004/6
Guided learning hours (GLH)	360
Total qualification time (TQT)	480
Minimum age	19
Qualification purpose	This qualification is designed to provide learners with the knowledge, skills and behaviours (KSBs) relevant to developing competence in cyber security. This qualification will provide employers with reliable evidence of a learner's attainment against occupational standard KSBs that form the minimum requirements for entry into occupation.
Grading	Not yet achieved/pass/merit/distinction
Assessment method	Internally assessed and externally quality assured portfolio of evidence.
Work/industry placement experience	Work/industry placement experience is not required.
Occupational standards	This qualification is mapped against the following occupational standard: ST0865: Cyber Security Technician (Level 3) Version 1.0 A mapping document is available on the qualification's page on the NCFE website.
UCAS	Please refer to the UCAS website for further details of points allocation and the most up-to-date information.
Regulation information	This is a regulated qualification. The regulated number for this qualification is 610/4004/6.
Funding	This qualification may be eligible for funding. For further guidance on funding, please contact your local funding provider.

Contents

Section 1: introduction

Please note this is a draft version of the Qualification Specification and is likely to be subject to change before the final version is produced for the launch of the qualification.

Centres must ensure they are using the most recent version of the Qualification Specification on the NCFE website.

Aims and objectives

This qualification aligns to knowledge, skills and behaviours (KSBs) in the ST0865: Cyber Security Technician (Level 3) Version 1.0 occupational standard.

This qualification aims to:

- focus on the study of the cyber security technician in the digital sector
- enable entry to the associated occupation, providing entry competence (further learning may be required in the workplace to reach full occupational competence)
- offer breadth and depth of study, incorporating a key core of knowledge
- provide opportunities to acquire a number of practical and technical skills

The objective of this qualification is to:

- enable entry to the associated occupation, providing entry competence (further learning may be required in the workplace to reach full occupational competence)

Support Handbook

This Qualification Specification must be used alongside the mandatory Support Handbook, which can be found on the NCFE website. This contains additional supporting information to help with planning, delivery and assessment.

This Qualification Specification contains all the qualification-specific information you will need that is not covered in the Support Handbook.

Guidance for entry and registration

This qualification is designed as an occupational entry technical qualification for adults.

Registration is at the discretion of the centre in accordance with equality legislation and should be made on the NCFE Portal.

There are no specific prior skills/knowledge a learner must have for this qualification. However, learners may find it helpful if they have already achieved a level 2 information technology (IT) qualification.

Centres are responsible for ensuring that all learners are capable of achieving the learning outcomes (LOs) and complying with the relevant literacy, numeracy, and health and safety requirements.

Learners registered on this qualification should not undertake another qualification at the same level, or with the same/a similar title, as duplication of learning may affect funding eligibility.

Achieving this qualification

To be awarded this qualification, learners are required to successfully achieve a pass grade in all **7 units** from the graded mandatory units.

Please refer to the list of units in appendix A or the unit summaries in section 2 for further information.

To achieve this qualification, learners must successfully demonstrate their achievement of all LOs of the units as detailed in this Qualification Specification.

Progression including job roles

Learners who achieve this qualification could progress to the following:

- employment:
    - cyber security administrator
    - cyber security technician
    - access control administrator
    - incident response technician
    - junior information security analyst
    - junior threat and risk analyst
    - junior penetration tester
- higher education

Progression to higher-level studies

Level 3 qualifications can support progression to higher-level study, which requires knowledge and skills different from those gained at levels 1 and 2. Level 3 qualifications enable learners to:

- apply factual, procedural and theoretical subject knowledge
- use relevant knowledge and methods to address complex, non-routine problems
- interpret and evaluate relevant information and ideas
- understand the nature of the area of study or work
- demonstrate an awareness of different perspectives and approaches
- identify, select and use appropriate cognitive and practical skills
- use appropriate research to inform actions
- review and evaluate the effectiveness of their own methods

Resource requirements

There are no mandatory resource requirements for this qualification, but centres must ensure learners have access to suitable resources to enable them to cover all the appropriate LOs.

Realistic work environment (RWE) requirement/recommendation

The assessment of competence-based criteria should ideally be conducted within the workplace. However, in instances where this is not feasible, learners can be assessed in a realistic work environment (RWE) designed to replicate real work settings.

It is essential for organisations utilising an RWE to ensure it accurately reflects current and authentic work environments. By doing so, employers can be confident that competence demonstrated by a learner in an RWE will be translated into successful performance in employment.

In establishing an RWE, the following factors should be considered.

The work situation being represented is relevant to the competence requirements being assessed:

- the work situation should closely resemble the relevant setting
- equipment and resources that replicate the work situation must be current and available for use to ensure that assessment requirements can be met
- time constraints, resource access and information availability should mirror real conditions

The learner's work activities reflect those found in the work environment being represented, for example:

- interaction with colleagues and others should reflect expected communication approaches
- tasks performed must be completed to an acceptable timescale
- learners must be able to achieve a realistic volume of work as would be expected in the work situation being represented
- learners operate professionally with clear understanding of their work activities and responsibilities
- feedback from colleagues and others (for example customers, service users) is maintained and acted upon
- account must be taken of any legislation, regulations or standard procedures that would be followed in the workplace

How the qualification is assessed

Assessment is the process of measuring a learner's skill, knowledge and understanding against the standards set in a qualification.

This qualification is internally assessed and externally quality assured.

The assessment consists of one component:

- an internally assessed portfolio of evidence, which is assessed by centre staff and externally quality assured by NCFE (internal quality assurance must still be completed by the centre as usual)

Learners must be successful in this component to gain the Level 3 Technical Occupational Entry in Cyber Security (Diploma).

Learners who are not successful can resubmit work within the registration period; however, a charge may apply in cases where additional external quality assurance visits are required.

Unless otherwise stated in this specification, all learners taking this qualification must be assessed in English and all assessment evidence presented for external quality assurance must be in English.

Internal assessment

We have created some sample tasks for the seven internally assessed units, which can be found within a separate document in the member's area of the NCFE website. These tasks are not mandatory. You can contextualise these tasks to suit the needs of your learners to help them build up their portfolio of evidence. The tasks have been designed to cover all LOs for seven units and provide opportunities for stretch and challenge. For further information about contextualising the tasks, please contact the Provider Development team.

Each learner must create a portfolio of evidence generated from appropriate assessment tasks to demonstrate achievement of all the LOs associated with each unit. The assessment tasks should allow the learner to respond to a real-life situation that they may face when in employment. On completion of each unit, learners must declare that the work produced is their own and the assessor must countersign this.

There is compensation within the internally assessed units as the grading descriptors are now based on LOs rather than specific assessment criteria (AC). This allows for increased professional judgement on the part of the assessor in terms of the learner's overall level of performance against the LOs.

If a centre needs to create their own internal assessment tasks, there are four essential elements in the production of successful centre-based assessment tasks; these are:

- ensuring the assessment tasks are meaningful with clear, assessable outcomes
- appropriate coverage of the content, LOs or assessment criteria (AC)
- having a valid and engaging context or scenario
- including sufficient opportunities for stretch and challenge for higher attainers

External quality assurance

Summatively assessed and internally quality assured grades for completed units must be submitted via the NCFE Portal, prior to an external quality assurance review taking place. Following the external quality assurance review, the unit grades will either be accepted and banked by your external quality assurer (EQA) or, if they disagree with the grades, they will be rejected. More detailed guidance on this process and what to do if your grades are rejected can be found in the Support Handbook and on the NCFE website.

Enquiries about results

All enquiries relating to learners' results must be submitted in line with our Enquiries and Appeals about Results and Assessment Decisions Policy, which is available on the NCFE website.

Not yet achieved grade

A result that does not achieve a pass grade will be graded as a not yet achieved grade. Learners may have the opportunity to resit. Learners may resubmit their assessment tasks, as many times as they require, if they have not successfully covered the criteria.

Grading information

Each unit of the qualification is graded using a structure of not yet achieved, pass, merit, distinction.

Grading internally assessed units

The grading descriptors for each unit have been included in the Qualification Specification. Grading descriptors have been written for each LO in a unit. Assessors must be confident that, as a minimum, all LOs have been evidenced and met by the learner. Assessors must make a judgement on the evidence produced by the learner to determine the grading decision for the unit.

If the learner has insufficient evidence to meet the pass criteria, a grade of not yet achieved must be awarded for the unit.

To achieve each unit the learner must:

- achieve all learning outcomes at a pass level to gain a pass grade
- achieve all learning outcomes at a pass level and at merit level to gain a merit grade
- achieve all learning outcomes at a pass, merit, and distinction level to gain a distinction grade

To achieve the qualification the learner must:

- pass all learning outcomes in all units

Centres must then submit each unit grade via the NCFE Portal. The grades submitted will be checked and confirmed through the external quality assurance process. This is known as ‘banking’ units. Once a learner’s grade has been banked, they are permitted one opportunity to revise and redraft their work; more detail on this process can be found in the Support Handbook.

The internal assessment component is based on performance of open-ended tasks that are assessed holistically against the grading descriptors to achieve a grade. Each unit of the qualification is internally assessed and will be allocated a weighting based on the guided learning hours (GLH) and a score based on the holistic grade.

There is compensation within the internally assessed units as the grading descriptors are now based on LOs rather than specific AC. All of the assessment points need to be evidenced in the learner’s portfolio, but the grade awarded is based on the standard of work for the LO as a whole. This allows for increased professional judgement on the part of the assessor in terms of the learner’s overall level of performance against the LOs.

Awarding the final grade

The final qualification grade is calculated by combining the scores for each unit. The total will then be converted into a grade based on the following fixed thresholds:

Units	Max	Pass (P)	Merit (M)	Distinction (D)
Unit 01 Cyber security concepts	14.3%	1	3	5
Unit 02 Cyber security threats, vulnerabilities and risks	14.3%	1	3	5
Unit 03 Risk and vulnerability assessment	14.3%	1	3	5
Unit 04 Incident response and disaster recovery	14.3%	1	3	5
Unit 05 Legislation and governance	14.3%	1	3	5

Unit 06 Cyber security measures	14.3%	1	3	5
Unit 07 Professional development in cyber security	14.3%	1	3	5

The table below shows how the accumulation of each unit grade is aggregated to form the overall qualification grade.

Total score	Grade
31-35	D
17-30	M
7-16	P
0-6	Not yet achieved

The final grade for the qualification is based on a structure of not yet achieved, pass, merit and distinction and will be issued to the centre by NCFE upon the centre claiming the learner's certificate on the NCFE Portal.

For further information on assessment, please refer to the User Guide to the External Quality Assurance Report, which can be found on the NCFE website.

NCFE does not anticipate any changes to our aggregation methods or any overall grade thresholds; however, there may be exceptional circumstances in which it is necessary to do so to secure the maintenance of standards over time. Therefore, overall grade thresholds published within this Qualification Specification may be subject to change.

Section 2: unit content and assessment guidance

This section provides details of the structure and content of this qualification.

The types of evidence listed are for guidance purposes only. Within learners' portfolios, other types of evidence are acceptable if all learning outcomes (LOs) are covered, and if the evidence generated can be internally and externally quality assured. For approval of methods of internal assessment other than portfolio building, please contact your external quality assurer (EQA).

The explanation of terms explains how the terms used in the unit content are applied to this qualification. This can be found in section 3.

Unit 01 Cyber security concepts

<table>
<tr><th colspan="4">Unit summary</th></tr>
<tr><td colspan="4">The learner will gain an understanding of cyber security and infrastructures. They will understand core terminology and the role of information assurance and governance (IAG). They will also investigate the importance of an effective security culture and the impact that an inadequate security culture may have on an organisation.</td></tr>
<tr><th colspan="4">Assessment</th></tr>
<tr><td colspan="4">This unit is internally assessed and externally quality assured.</td></tr>
<tr><td><b>Mandatory</b></td><td><b>Graded P/M/D</b></td><td><b>Level 3</b></td><td><b>45 GLH</b></td></tr>
</table>

Learning outcomes (LOs) The learner will:	**Assessment criteria (AC)**	**Pass** The learner will be able to:	**Merit** The learner will be able to:	**Distinction** The learner will show evidence of:
1. Understand the key concepts within cyber security	1.1 The key concepts and importance of cyber security: • CIA triad: ○ confidentiality ○ integrity ○ availability • IAAA: ○ identification ○ authentication ○ authorisation ○ accountability	Outline the concepts of cyber security (as identified in AC1.1).	Explain how the key core concepts in cyber security are used by an organisation to ensure the safety of data and assets.	Analyse the importance of cyber security and its key concepts for an organisation to ensure its safety of data and assets.
	1.2 The use of core terminology in cyber security: • assurance • reliability • non-repudiation	Identify the use of core terminology in cyber security (as identified in AC1.2).		

	• access control • threat • vulnerability • risk • security breach • information security • attack vectors • attack surface			
	1.3 The role of information assurance and governance (IAG): • to guide the development and improvement of policies and processes • to support the auditing of policies and processes • to provide confirmation of compliance (for example, with International Organization of Standardization (ISO) standards)	Outline the role of IAG (as identified in AC1.3).	Explain how IAG plays an important role in the development, improvement and auditing of policies and processes, ensuring legal and organisational compliance.	Evaluate the importance IAG it plays in the development, improvement and auditing of policies and processes, ensuring legal and organisational compliance.
2. Understand effective cyber security culture	2.1 The influence of organisational structures on cyber security culture:	Outline the influence of organisational structures on cyber security culture (as identified in AC2.1).	Discuss how the influence of organisational structures impact maintaining an effective cyber security	Evaluate the importance of building and maintaining an effective security culture for

	• stakeholders (for example, internal or external) • organisational types (for example, public or private)		culture that protects the confidentiality of an organisations' information.	different organisations and the stakeholders involved.
	2.2 The importance of maintaining an effective cyber security culture in protecting the confidentiality of an organisations' information	Identify the importance of maintaining an effective cyber security culture in protecting the confidentiality of an organisations' information.		
	2.3 The components and importance of an effective security culture	Outline the components and importance of an effective security culture.	Explain the components and techniques used to build and maintain an effective security culture and the impact of not adhering to this.	
	2.4 The techniques used to build and maintain an effective security culture	Identify techniques used to building and maintain an effective security culture.		
	2.5 The impact of an inadequate cyber security culture on an organisation (for example, unauthorised distribution or loss of data, reputational damage)	Outline the impact of an inadequate cyber security culture on an organisation.		
3. Understand secure infrastructure and cloud environments	3.1 The components of a secure infrastructure within an organisation: • hardware	Outline the components of a secure infrastructure within an organisation (as identified in AC3.1).	Describe the components of securing infrastructure and cloud environments within an organisation.	Analyse the benefits that secure infrastructure and cloud environments provide to cyber security.

	• software • operating systems (OSs) • network resources			
	3.2 The components of cloud environments: • Infrastructure as a Service (IaaS) • Platform as a Service (PaaS) • Software as a Service (SaaS)	Outline the components of cloud environments (as identified in AC3.2).		

Unit 02 Cyber security threats, vulnerabilities and risks (D/651/1096)

Unit summary			
The learner will understand cyber security threats, suspicious activities and potential breaches. They will understand and be able to perform threat intelligence gathering using reliable sources. The learner will also understand evolving cyber security issues and how these can impact critical national infrastructure and control systems. They will go on to understand digital information assets and will be able to maintain an inventory of digital information systems.			
Assessment			
This unit is internally assessed and externally quality assured.			
Mandatory	**Graded P/M/D**	**Level 3**	**54 GLH**

Learning outcomes (LOs) The learner will:	**Assessment criteria (AC)**	**Pass** The learner will be able to:	**Merit** The learner will be able to:	**Distinction** The learner will show evidence of:
1. Understand cyber security threats and perform intelligence gathering	1.1 The function and features of the threat intelligence lifecycle	Outline the function and features of the threat intelligence lifecycle.	Explain the role of the threat intelligence lifecycle, clearly identifying the purpose of each phase.	Analyse potential threats and reconnaissance techniques, considering their motivations and impacts, and how the threat intelligence cycle can be used to anticipate and mitigate these threats.
	1.2 How to use reliable sources to contribute to threat intelligence gathering tasks (for example, MITRE ATT&CK®)	Outline how to use reliable sources to contribute to threat intelligence gathering tasks.		
	1.3 The impact of threats on an organisation (for example, financial, data loss)	Identify the impact of threats on an organisation.	Explain the motivations of threat actors and the impact of different types of threats on organisations.	
	1.4 Types of threats and the methods used to identify them (for example, social engineering,	Identify the types of threats and the methods used to identify them.		

	ransomware, zero-day, commodity threat)			
	1.5 The types and motivations of threat actors: • nation state • script kiddies • cyber criminals • terrorist organisations • insiders • hacktivists	Identify the types and motivations of threat actors (as identified in AC1.5).		
	1.6 The application of network reconnaissance techniques to identify threats: • indicators of compromise (IOCs) from external threat intelligence sources • use of tools to scan and analyse network traffic • monitoring: ○ unusual volume of network traffic ○ repeated attempts to access systems ○ alerts from end points	Summarise the application of network reconnaissance techniques to identify threats (as identified in AC1.6).	Compare a range of network reconnaissance techniques and how these can be used to assist threat identification.	

	○ abnormal user behaviour ○ unexpected system changes			
	1.7 Perform routine threat intelligence gathering tasks using reliable sources	Demonstrate the ability to perform routine threat intelligence gathering tasks using reliable sources.		
2. Understand suspicious activities and potential breaches	2.1 The characteristics of unusual security activity: • suspicious user behaviour (for example, brute force attack) • suspicious device behaviour (for example, unusual network activity) • unauthorised system changes (for example, changes to network configuration) • malware activity (for example, IOCs)	Outline the characteristics of unusual security activity (as identified in AC2.1).	Explain how security procedures and training can be effective to increase awareness of a range of unusual security activity.	Evaluate the importance of understanding of how to identify unusual security activity and training methods for raising awareness with stakeholders.
	2.2 Follow information security procedures to maintain cyber security resilience	Demonstrate the ability to follow an information security procedure to maintain cyber security resilience.		
	2.3 Develop information security training and	Demonstrate the ability to develop information security		

	awareness resources to support good cyber security practice	training and awareness resources to support good cyber security practice.		
	2.4 Monitor the effectiveness of security awareness and training resources	Demonstrate the ability to monitor the effectiveness of security awareness and training resources.		
3. Understand evolving cyber security issues	3.1 The types of cyber security issues and how these are evolving (for example, artificial intelligence (AI), quantum computing)	Identify types of cyber security issues and how these are evolving.	Explain how evolving cyber security risks and emerging technologies could impact critical national infrastructure and control systems.	Evaluate the threats that evolving cyber security risks and emerging technology may have on critical national infrastructure and control systems.
	3.2 How evolving cyber security issues can impact critical national infrastructure and control systems: • military and national defence (for example, leaking of classified information) • healthcare (for example, compromised confidentiality, ability to treat patients) • transport (for example, disruption	Identify how evolving cyber security issues can impact critical national infrastructure and control systems (as identified in AC3.2).		

	to airlines, rail, smart motorways) • communication (for example, mass loss of service, interruptions to business and society) • utilities (for example, water and sanitation, energy sources) • supply chain (for example, production of food) • finance (for example, disruption or failure of payment transactions) • operational technologies (OT) (for example, disruption to Supervisory Control and Data Acquisition (SCADA))			
	3.3 The importance of the threat landscape and the associated risks to internet of things (IoT) devices (for example,	Outline the importance of the threat landscape and the associated risks to IoT devices.	Explain the importance of the threat landscape and the associated risks to IoT devices.	Evaluate the importance of the threat landscape and the associated risks to IoT devices.

	privacy, compromising other devices on network, trustworthy brand)			
4. Understand and maintain digital information systems	4.1 The types of digital information assets and how they are securely stored and accessed in a controlled environment: • systems • services • devices • data storage	Outline of the types of digital information assets (as identified in AC4.1) and how they are securely stored and accessed in a controlled environment.	Compare a range of methods that may be implemented for storing and managing digital information assets and how they are managed across cloud services.	Evaluate a range of methods for storing and managing digital information assets, assessing their effectiveness and suitability across different cloud services.
	4.2 How digital information assets are managed across cloud services	Outline how digital information assets are managed across cloud services.		
	4.3 The importance and application of maintaining a digital information asset inventory (for example, compliance with ISO/IEC 27001 standard)	Outline the importance and application of maintaining a digital information asset inventory.	Discuss the importance of maintaining digital information asset inventory and use of secure digital information asset disposal.	Evaluate the importance of maintaining an accurate inventory of digital information assets and implementing secure methods for their disposal to mitigate data loss and ensure compliance.
	4.4 The importance and use of secure digital information asset disposal (for example, data sanitisation)	Outline the importance and use of secure digital information asset disposal.		

	4.5 Maintain an inventory of digital information systems, services, devices and data storage	Demonstrate the ability to maintain an inventory of digital information systems, services, devices and data storage.		

Unit 03 Risk and vulnerability assessment (F/651/1097)

Unit summary			
The learner will understand common vulnerability exposures and the impact they can have on an organisation. They will understand the process of risk management and be able to identify and categorise threats, vulnerabilities and risks. The learner will also be able to identify when and how to escalate information security events and how to use tools and techniques to evaluate vulnerability assessments. They will understand how to make recommendations based on evidence from a vulnerability assessment tool and will be able to evaluate these results. They will go on to understand computer forensic principles and the importance of ensuring evidence is not contaminated or compromised.			
Assessment			
This unit is internally assessed and externally quality assured.			
Mandatory	**Graded P/M/D**	**Level 3**	**54 GLH**

Learning outcomes (LOs) The learner will:	**Assessment criteria (AC)**	**Pass** The learner will be able to:	**Merit** The learner will be able to:	**Distinction** The learner will show evidence of:
1. Understand cyber security vulnerabilities	1.1 Common vulnerability exposures and the impact these can have on an organisation: • software misconfiguration (for example, authentication bypass, data loss) • broken access control and authentication (for example, unauthorised access) • sensitive data exposure (for	Outline common vulnerability exposures (as identified in AC1.1) and the impact these can have on an organisation.	Compare a wide range of common vulnerability exposures, clearly identifying the impact each of these may have on an organisation.	Evaluate the impact cyber security vulnerabilities can have on an organisation.

	example, reputational damage, fines) • injection vulnerabilities (for example, remote code execution, Denial of Service (DoS)) • using components with known vulnerabilities (for example, software security weakness) • insufficient logging and monitoring (for example, unacknowledged persistent threat) • security misconfiguration (for example, lack of network restrictions or anti-virus protection) • incorrect cross-site validation (for example, session hijacking)			
2. Understand and categorise cyber security risks for escalation	2.1 The process of risk management and risk assessment to	Outline of the process of risk management and risk assessment (as identified in	Explain how risk assessments are used to categorise vulnerabilities	Analyse the risk management process and risk assessment techniques

	categorise threats, vulnerabilities and risks: • identification of the scope of the risk assessment • assessment of the risk using a scoring matrix (for example, probability versus impact) • categorisation of the risk rating (for example, apply a red, amber, green (RAG) rating) • recording, responding or escalating as appropriate • completion of a business impact analysis	AC2.1) to categorise threats, vulnerabilities and risks.	and threats through the application of a detailed and accurate risk matrix and risk register.	used to categorise and prioritise cybersecurity risks, threats, and vulnerabilities.
	2.2 Categorise threats, vulnerabilities and risks in preparation for response or escalation	Demonstrate the ability to identify and categorise threats, vulnerabilities and risks in preparation for response or escalation.		
	2.3 Perform digital information risk assessments	Demonstrate the ability to perform digital information risk assessments.		
	2.4 Use own initiative to identify when and how	Demonstrate the ability to identify when and how to		

	to escalate information security events in accordance with relevant procedures and standards	escalate information security events in accordance with relevant procedures and standards.		
3. Understand and evaluate vulnerability assessments	3.1 The considerations for a vulnerability assessment scope: • networks • computers • servers • business units • applications	Identify the considerations for a vulnerability assessment scope (as identified in AC3.1).	Describe key considerations when defining the scope of a vulnerability assessment, and the tools and techniques used to conduct the evaluation.	Evaluate the planning, execution, and outputs of a vulnerability assessment, considering the effectiveness of chosen tools and how the results may inform further actions.
	3.2 The use of tools and techniques to evaluate vulnerability assessments: • Common Vulnerabilities and Exposures (CVE) • Common Vulnerability Scoring System (CVSS)	Identify the use of tools and techniques to evaluate vulnerability assessments (as identified in AC3.2).		
	3.3 The scope and objectives of vulnerability assessment	Demonstrate the ability to define the scope and objectives of a cyber security vulnerability assessment.		
	3.4 How to make recommendations based on evidence from	Identify how to make recommendations based on evidence from vulnerability	Describe how recommendations can be made based on the severity	

	vulnerability assessment tools: • severity of the vulnerability • potential impact and risk on business • availability of resources (for example, time, finances) • acceptance of risk • potential mitigations • scope of mitigation projects	assessment tools (as identified in AC3.4).	and impact of the vulnerability with consideration for potential mitigation techniques and resource constraints.	
	3.5 How to interpret the results of a cyber security vulnerability assessment	Demonstrate the ability to interpret the results of a cyber security vulnerability assessment.		
4. Understand computer forensics	4.1 The concept of computer forensic principles: • identification (for example, the evidence that is presented, where it is stored and how it can be accessed) • preservation (for example, isolating, securing and	Outline the concept of computer forensic principles (as identified in AC4.1).	Explain the concepts of computer forensic principles with a focus on the key elements (as identified in AC4.1) to ensure that evidence is not compromised.	Evaluate the concept of computer forensics and the importance of maintaining evidence integrity to prevent contamination or compromise during collection, analysis, and storage.

	preserving evidence) • analysis (for example, evidence-based conclusions) • documentation (for example, retained in line with legal retention periods) • presentation (for example, evidence presented to law enforcement for further investigation)			
	4.2 The importance of ensuring evidence is not contaminated or compromised (for example, continuity of evidence to support court cases)	Outline the importance of ensuring evidence is not contaminated or compromised.		

Unit 04 Incident response and disaster recovery (H/651/1098)

Unit summary			
The learner will understand the phases of the incident response lifecycle. They will understand the use of reports and will be able to create draft management reports to meet requirements. They will understand the importance of maintaining an up-to-date cyber security incident log and will be able to create cyber security event information documents and preserve evidence. The learner will go on to understand how monitoring systems are used to identify information security events and will be able to monitor and report these events.			
Assessment			
This unit is internally assessed and externally quality assured.			
Mandatory	**Graded P/M/D**	**Level 3**	**54 GLH**

Learning outcomes (LOs) The learner will:	**Assessment criteria (AC)**	**Pass** The learner will be able to:	**Merit** The learner will be able to:	**Distinction** The learner will show evidence of:
1. Understand and create incident response documentation	1.1 The phases and application of the incident response lifecycle: • preparation • detection and analysis • containment • eradication and recovery • post-event activity and lessons learned	Outline the phases and the application of the incident response lifecycle (as identified in AC1.1).	Explain the phases of the incident response lifecycle and the importance reporting plays in the process, highlighting where reporting plays an important part in the process.	Analyse the incident response lifecycle, highlighting the significance of timely and accurate reporting throughout each stage.
	1.2 The application of exception reporting: • reporting of incidents (for example, breaches	Outline the application of exception reporting.		

	of information security policy)			
	1.3 The application of management reporting: - regular reporting (for example, recent events, threat landscape)	Outline the application of management reporting.		
	1.4 Create draft information management reports using standard formats to meet requirements	Demonstrate the ability to create draft information management reports using standard formats to meet requirements.		
2. Understand and create cyber security incident information documentation	2.1 The importance of maintaining an up-to-date cyber security incident log as part of a chain of evidence	Outline the importance of maintaining an up-to-date cyber security incident log as part of a chain of evidence.	Discuss why it is important to maintain an up-to-date cyber incident log and how this forms part of the chain of evidence.	Evaluate the importance of maintaining an up-to-date cyber incident log as part of a chain of evidence.
	2.2 Create cyber security event information documents and preserve evidence to meet requirements	Demonstrate the ability to create a cyber security event information document and preserve evidence to meet requirements.		
3. Understand and monitor systems to identify information security events	3.1 The application of monitoring systems to identify information security events (for example, monitoring alerts, checking logs)	Outline how monitoring systems (as identified in AC3.1) are used to identify information security events.	Explain how monitoring systems are effectively used within an organisation as a method to check for security events.	Analyse the importance of implementing monitoring systems to identify, track, and respond to security events.
	3.2 Monitor and report information security	Demonstrate the ability to monitor and report		

	events to meet requirements	information security events to meet requirements.		
4. Understand disaster prevention and recovery	4.1 The use of disaster prevention and recovery methods to support continuity of service planning: • disaster recovery plan (DRP) • business continuity plan (BCP)	Outline the use of disaster prevention and recovery methods (as identified in AC4.1) to support the continuity of service planning.	Discuss the use of disaster prevention and recovery methods to support continuity of service planning.	Evaluate the effectiveness of disaster prevention and recovery methods in ensuring continuity of service.
	4.2 The purpose and use of secure on-site and off-site backup and recovery techniques (for example, incremental, air-gapped)	Outline the purpose and use of secure on-site and off-site backup and recovery techniques.		

Unit 05 Legislation and governance (J/651/1099)

Unit summary			
The learner will understand organisational security governance and the value of information security management systems (ISMSs). They will understand and be able to review and comment upon cyber security policies, procedures, standards and guidelines. The learner will go on to understand the use of legislation to support cyber security whilst being able to maintain knowledge of legislation and industry standards relating to cyber security. The learner will also understand ethical considerations when processing and storing data, and codes of conduct within cyber security. They will understand the purpose of cyber security audit requirements and will be able to document audit requirements and perform cyber security compliance checks.			
Assessment			
This unit is internally assessed and externally quality assured.			
Mandatory	**Graded P/M/D**	**Level 3**	**54 GLH**

Learning outcomes (LOs) The learner will:	**Assessment criteria (AC)**	**Pass** The learner will be able to:	**Merit** The learner will be able to:	**Distinction** The learner will show evidence of:
1. Understand information security governance	1.1 The purpose of organisational security governance: • provides a framework for managing compliance with legislation, standards, policies and processes • supports risk management	Outline the purpose of organisational security governance (as identified in AC1.1).	Explain the purpose of organisational security governance.	Evaluate information security governance and its impact on organisational security.
2. Understand and review cyber security policies	2.1 The value of an information security management system (ISMS) to support	Outline the value of an ISMS to support compliance with cyber security standards (as identified in AC2.1).	Explain the benefits an ISMS offers by providing a framework to managing security risks, paying	Evaluate the importance of an ISMS system to ensure compliance with cyber security standards.

	compliance with cyber security standards: • people • processes • technology		attention to compliance, policies and procedures.	
	2.2 How an ISMS system supports compliance with cyber security standards (for example, International Standards Organisation (ISO) standards)	Identify how an ISMS system supports compliance with cyber security standards.		
	2.3 Review and comment upon cyber security policies, procedures, standards and guidelines	Demonstrate the ability to review and comment upon cyber security policies, procedures, standards and guidelines.		
3. Understand knowledge of legislation relating to cyber security	3.1 The use of current legislation and standards to support cyber security: • Data Protection Act 2018 • Regulation of Investigatory Powers Act 2000 • Human Rights Act 1998 • Computer Misuse Act 1990	Outline the use of current legislation and standards to support cyber security (as identified in AC3.1).	Discuss how current legislation and standards are used to guide cyber security within an organisation including methods used to maintain currency of knowledge.	Analyse how current legislation and standards influence cyber security within an organisation.

	• Freedom of Information Act 2000 • Official Secrets Act 1989 • Wireless Telegraphy Act 2006 • Payment Card Industry Data Security Standard (PCI DSS)			
	3.2 How to maintain knowledge of legislation and industry standards relating to cyber security	Outline how to maintain knowledge of legislation and industry standards relating to cyber security.		
4. Understand ethical considerations and codes of conduct	4.1 Ethical considerations when processing and storing data: • consent • contract • legal obligations • vital interests • public interest • legitimate interests	Outline the ethical considerations when processing and storing data (as identified in AC4.1).	Describe how codes of conduct may support with ethical considerations.	Analyse the extent that codes of conduct support ethical considerations.
	4.2 The attributes of ethical codes of conduct within cyber security: • UK Cyber Security Council Code of Ethics	Identify the attributes of ethical codes of conduct within cyber security (as identified in AC4.2).		

	• British Computer Society (BCS) Code of Conduct • Ethics for Incident Response and Security Teams (EthicsfIRST)			
5. Understand cyber security policies and compliance	5.1 The purpose and application of common information security policies: • acceptable use policy • incident management policy • bring your own device (BYOD) policy • access control policy • social media policy • password policy • patch management policy • anti-virus policy • information security policy • data classification and handling policy • IT asset disposal policy	Outline the purpose and application of common information security policies (as identified in AC5.1).	Discuss how policies are applied within an organisation and the techniques used to ensure cyber security compliance.	Evaluate the extent to which information security policies contribute to ensuring cyber security compliance, focusing on their effectiveness in mitigating risks, meeting requirements, and safeguarding assets.

	5.2 The concept of cyber security compliance (for example, compliance with legal or internal policy requirements)	Outline the concept of cyber security compliance.		
	5.3 The use of compliance monitoring techniques (for example, audits)	Identify the use of compliance monitoring techniques.		
6. Understand cyber security auditing and perform compliance checks	6.1 The purpose and application of cyber security audit requirements in line with organisational procedures (for example, scoping, planning)	Outline the purpose and application of cyber security audit requirements in line with organisational procedures.	Discuss the importance of cyber security audits and the techniques used to ensure these are conducted in line with organisational procedures to ensure these are in an appropriate format.	Evaluate the benefits of auditing and compliance and the techniques used within an organisation.
	6.2 The importance of obtaining and documenting evidence in an appropriate form for review by an internal or external auditor	Identify the importance of obtaining and documenting evidence in an appropriate form for review by an internal or external auditor.		
	6.3 Document audit requirements and collate relevant information from log files, incident reports and appropriate data sources	Demonstrate the ability to document audit requirements and collate relevant information from log files, incident reports and appropriate data sources.		
	6.4 Perform cyber security compliance checks	Demonstrate the ability to perform cyber security compliance checks.		

Unit 06 Cyber security measures (T/651/1100)

Unit summary			
The learner will understand service desk delivery as well as how and when to escalate a security ticket. They will go on to understand the types of cyber security controls, measures and tools, and will be able to maintain information security controls and measures. The learner will understand cryptographic techniques and the use of digital certificates. They will also understand, identify and access management and will be able to review and modify access rights to digital information systems, services, devices or data.			
Assessment			
This unit is internally assessed and externally quality assured.			
Mandatory	**Graded P/M/D**	**Level 3**	**54 GLH**

Learning outcomes (LOs) The learner will:	**Assessment criteria (AC)**	**Pass** The learner will be able to:	**Merit** The learner will be able to:	**Distinction** The learner will show evidence of:
1. Understand service desk delivery	1.1 The purpose and use of service desk delivery in resolving security issues	Outline the purpose and use of service desk delivery in resolving security issues.	Describe the purpose and use of service desk delivery in resolving security issues.	Analyse the importance of service desk delivery in resolving issues including accurate communication when escalating tickets.
	1.2 How and when to escalate a security ticket to a higher level	Identify how and when to escalate a security ticket to a higher level.	Describe how and when to escalate a security ticket to a higher level.	
	1.3 The importance of communicating accurately and appropriately during escalation (for example, technical or non-technical audience)	Outline the importance of communicating accurately and appropriately during escalation.	Explain the importance of communicating accurately and appropriately during escalation.	
2. Understand, maintain and install cyber security controls	2.1 The types of cyber security controls: • physical (for example, door access)	Outline the types of cyber security controls (as identified in AC2.1).	Describe the various types of security control along with the associated measures and tools used to implement them effectively.	Analyse the different types of security controls and the effectiveness of associated measures and tools in

	• procedural (for example, acceptable use policy, vulnerability management policy, security incident response procedure) • technical (for example, firewalls, applications, user access control)			addressing specific cybersecurity threats.
	2.2 The application of common cyber security measures and tools: • patching • software updates • access control • password management • firewalls • security incident and event management (SIEM) tools • protection tools: ○ anti-virus ○ anti-malware ○ anti-spam • technical management and monitoring tools (for	Outline the application of common cyber security measures and tools (as identified in AC2.2).		

	example, cloud security posture management (CSPM), cloud-native application protection platform (CNAPP))			
	2.3 Maintain information security controls and measures	Demonstrate the ability to maintain information security controls and measures.		
	2.4 Use a structured approach to manage and assess the validity of security requests from a range of stakeholders	Demonstrate the ability to use a structured approach to manage and assess the validity of security requests from a range of stakeholders.		
	2.5 Use technical procedures to install and maintain technical security controls	Demonstrate the ability to use technical procedures to install and maintain technical security controls.		
3. Understand cryptography and digital certificates	3.1 The purpose of cryptography in cyber security: • eavesdropping of information • prevention of tampering of information to ensure integrity of data	Outline the purpose of cryptography in cyber security (as identified in AC3.1).	Explain the purpose of cryptography in cyber security and the different types and techniques used to ensure confidentiality.	Evaluate the effectiveness of cryptography and digital certificates in maintaining a secure and trustworthy environment.

	• assurance of authenticity of information • secure storage of sensitive data			
	3.2 Types of cryptographic techniques in cyber security: • hashing • symmetric encryption (for example, Blowfish, Twofish) • asymmetric encryption (for example, Rivest Shamir Adleman (RSA), Diffie-Hellman)	Outline the types of cryptography in cyber security (as identified in AC3.2).		
	3.3 The use of digital certificates: • to verify the identity of users • to verify servers • to sign data to prove authenticity • to secure communications in transit	Outline the use of digital certificates (as identified in AC3.3).	Explain the reasons for using digital certificates and the tools used to manage these.	

	3.4 The purpose of certificate management tools: • generating certificate signing requests • signing new certificates • secure management of keys • tracking expired certificates • revoking compromised certificates	Outline the purpose of certificate management tools (as identified in AC3.4).		
4. Understand and modify access controls	4.1 The principles of identity and access management: • authentication • authorisation and federation	Outline the principles of identity and access management (as identified in AC4.1).	Discuss the role access management and access controls mechanisms play in securing systems and data.	Evaluate the significance of access management and access control practices in maintaining robust cyber security.
	4.2 The types and application of access control: • mandatory access control (MAC) • discretionary access control (DAC) • attribute-based access control (ABAC)	Outline the types and application of access control (as identified in AC4.2).		

	• role-based access control (RBAC) • rule-based access control (RuBAC)			
	4.3 The relationship between privacy and access rights and access control	Outline the relationship between privacy and access rights and access control.		
	4.4 Review and modify access rights to digital information systems, services, devices or data	Demonstrate the ability to review and modify access rights to digital information systems, services, devices or data.		

Unit 07 Professional development in cyber security (Y/651/1101)

Unit summary			
The learner will understand digital transformation and its impact on cyber security occupations. They will investigate the skill requirements for cyber security occupations and how current regulatory requirements influence these occupations. The learner will understand learning techniques and how to review own development needs to keep up to date with emerging technologies and trends within cyber security. The learner will go on to understand multidisciplinary teams and will be able to apply communication skills and technical and non-technical terminology to share information. They will understand the value of working independently and how to manage time to meet deadlines.			
Assessment			
This unit is internally assessed and externally quality assured.			
Mandatory	**Graded P/M/D**	**Level 3**	**45 GLH**

Learning outcomes (LOs) The learner will:	**Assessment criteria (AC)**	**Pass** The learner will be able to:	**Merit** The learner will be able to:	**Distinction** The learner will show evidence of:
1. Understand digital transformation	1.1 The impact of digital transformation (for example, new IT system) on cyber security occupations and within an overall business context: • customer issues and problems • business value • brand awareness • cultural/diversity awareness • internal and external stakeholders: ○ user experience ○ accessibility	Outline the impact of digital transformation on cyber security roles and business operations.	Discuss ways in which the impact of digital transformation can be managed effectively, ensuring minimal disruption.	Evaluate the impact of digital transformation on cyber security occupations and its broader impact on business operations.

	○ level of technical knowledge			
2. Understand cyber security occupations and regulatory requirements	2.1 The skill requirements for different cyber security occupations and how these fit into the wider digital landscape	Outline the skill requirements for different cyber security occupations and how these fit into the wider digital landscape.	Compare different cyber security occupations, considering the influence regulatory requirements may have on them and how these may evolve over time.	Analyse the impact of regulatory requirements on various cyber security occupations and how these roles may evolve in response to this.
	2.2 The influence of current regulatory requirements on cyber security occupations	Outline the influence of current regulatory requirements on cyber security occupations.		
	2.3 How cyber security regulations may evolve in the future	Identify how cyber security regulations may evolve in the future.		
3. Understand learning techniques and sources of knowledge and review own development needs	3.1 How learning techniques (for example, evaluation and reflection) contribute to continuing professional development (CPD) of cyber security occupations	Outline how learning techniques contribute to CPD of cyber security occupations.	Compare different types of learning techniques that contribute to CPD in the field of cyber security.	Evaluate the effectiveness of different types of learning techniques that contribute to CPD in the field of cyber security.
	3.2 A range of sources of knowledge and verified information applicable to cyber security occupations (for example, professional networks, academic publications)	Identify a range of sources of knowledge and verified information applicable to cyber security occupations.	Describe a range of sources of knowledge and verified information used to support own professional development in the field of cyber security.	Analyse a range of sources of knowledge and verified information used to support own professional development in the field of cyber security.

	3.3 Review own development needs to keep up to date with emerging technologies and trends within cyber security	Demonstrate the ability to review own development needs to keep up to date with emerging technologies and trends within cyber security.		
4. Understand multidisciplinary teams and apply communication skills to share information	4.1 The purpose of a multidisciplinary team	Outline the purpose of a multidisciplinary team.	Explain the benefits and limitations of implementing multidisciplinary teams using relevant working examples.	Evaluate how effectively multidisciplinary teams can address cyber security challenges.
	4.2 How the roles within a multidisciplinary team are identified	Outline how the roles within a multidisciplinary team are identified.		
	4.3 The value of communication within multidisciplinary teams	Outline the value of communication within multidisciplinary teams.		
	4.4 Apply communication skills using appropriate technical and non-technical terminology to share information with stakeholders (for example, within a multidisciplinary team)	Demonstrate the ability to apply communication skills using appropriate technical and non-technical terminology to share information with stakeholders.	Explain the benefits and limitations of applying communication skills using appropriate technical and non-technical terminology to share information with stakeholders.	Evaluate the effective application of communication skills using appropriate technical and non-technical terminology; teams can address cyber security challenges.
5. Understand independent working, time management and stakeholder engagement	5.1 The value of working independently and taking responsibility for own actions	Outline the value of working independently and taking responsibility for own actions.	Describe how to work independently, manage own time to meet deadlines and manage stakeholder expectations.	Evaluate the benefits of working independently, manage time effectively to meet deadlines, and handle stakeholder expectations in cyber security projects.
	5.2 How to manage own time to meet deadlines and manage stakeholder expectations	Outline how to manage own time to meet deadlines and manage stakeholder expectations.		

	5.3 The importance of treating all stakeholders fairly and with respect without bias or discrimination	Outline the importance of treating all stakeholders fairly and with respect without bias or discrimination.	Explain the importance of treating all stakeholders fairly and with respect without bias or discrimination.	Evaluate the importance of treating all stakeholders fairly and with respect without bias or discrimination.

NCFE assessment strategy

The key requirements of the assessment strategies or principles that relate to units in this qualification are summarised below.

The centre must ensure that individuals undertaking assessor or quality assurer roles within the centre conform to the assessment requirements for the unit they are assessing or quality assuring.

Knowledge LOs

- assessors will need to be both occupationally knowledgeable and qualified to make assessment decisions
- internal quality assurers (IQAs) will need to be both occupationally knowledgeable and qualified to make quality assurance decisions

Skills LOs

- assessors will need to be both occupationally competent and qualified to make assessment decisions
- IQAs will need to be both occupationally knowledgeable and qualified to make quality assurance decisions

The centre with whom the learners are registered will be responsible for making all assessment decisions. Assessors must be **contracted** to work directly with the centre, contributing to all aspects of standardisation. The centre must ensure a process of training is followed, including during induction and quality assurance activities. Occupationally competent and qualified assessors from the centre must use direct observation to assess practical skills-based outcomes.

Section 3: explanation of terms

This table explains how the terms used at **level 3** in the unit content are applied to this qualification (not all verbs are used in this qualification).

Analyse	Break down the subject into separate parts and examine each part. Show how the main ideas are related and why they are important. Reference to current research or theory may support the analysis.
Apply	Explain how existing knowledge can be linked to new or different situations in practice.
Clarify	Explain the information in a clear, concise way.
Classify	Organise according to specific criteria.
Collate	Collect and present information arranged in sequential or logical order.
Compare	Examine the subjects in detail and consider the similarities and differences.
Critically compare	This is a development of ‘compare’ where the learner considers the positive aspects and limitations of the subject.
Consider	Think carefully and write about a problem, action or decision.
Create	Make or produce an artefact as required.
Demonstrate	Show an understanding by describing, explaining or illustrating using examples.
Describe	Write about the subject giving detailed information in a logical way.
Develop (a plan/idea)	Expand a plan or idea by adding more detail and/or depth of information.
Diagnose	Identify the cause based on valid evidence.
Differentiate	Identify the differences between two or more things.
Discuss	Write a detailed account giving a range of views or opinions.
Distinguish	Explain the difference between two or more items, resources, pieces of information.
Draw conclusions	Make a final decision or judgement based on reasons.
Estimate	Form an approximate opinion or judgement using previous knowledge or considering other information.

Evaluate	Examine strengths and weaknesses, arguments for and against and/or similarities and differences. Judge the evidence from the different perspectives and make a valid conclusion or reasoned judgement. Reference to current research or theory may support the evaluation.
Explain	Provide detailed information about the subject with reasons showing how or why. Responses could include examples to support these reasons.
Extrapolate	Use existing knowledge to predict possible outcomes that might be outside the norm.
Identify	Recognise and name the main points accurately. (Some description may also be necessary to gain higher marks when using compensatory marking).
Implement	Explain how to put an idea or plan into action.
Interpret	Explain the meaning of something.
Judge	Form an opinion or make a decision.
Justify	Give a satisfactory explanation for actions or decisions.
Perform	Carry out a task or process to meet the requirements of the question.
Plan	Think about and organise information in a logical way using an appropriate format.
Provide	Identify and give relevant and detailed information in relation to the subject.
Reflect	Learners should consider their actions, experiences or learning and the implications of this for their practice and/or professional development.
Review and revise	Look back over the subject and make corrections or changes.
Select	Make an informed choice for a specific purpose.
Show	Supply evidence to demonstrate accurate knowledge and understanding.
State	Give the main points clearly in sentences or paragraphs.
Summarise	Give the main ideas or facts in a concise way.
Test	Complete a series of checks utilising a set procedure.

Section 4: support

Support materials

The following support materials are available to assist with the delivery of this qualification and are available on the NCFE website:

- learning resources
- Qualification Factsheet
- Sample Assessment Materials

Other support materials

The resources and materials used in the delivery of this qualification must be age-appropriate and due consideration should be given to the wellbeing and safeguarding of learners in line with your institute's safeguarding policy when developing or selecting delivery materials.

Products to support the delivery of this qualification may be available. For more information about these resources and how to access them, please visit the NCFE website.

Reproduction of this document

Reproduction by approved centres is permissible for internal use under the following conditions:

- you may copy and paste any material from this document; however, we do not accept any liability for any incomplete or inaccurate copying and subsequent use of this information
- the use of PDF versions of our support materials on the NCFE website will ensure that correct and up-to-date information is provided to learners
- any photographs in this publication are either our exclusive property or used under licence from a third party:
    - they are protected under copyright law and cannot be reproduced, copied or manipulated in any form
    - this includes the use of any image or part of an image in individual or group projects and assessment materials
    - all images have a signed model release

Contact us

NCFE
Q6
Quorum Park
Benton Lane
Newcastle upon Tyne
NE12 8BT

Tel: 0191 239 8000*
Fax: 0191 239 8001
Email: customersupport@ncfe.org.uk
Website: www.ncfe.org.uk

Version 1.0 August 2025
Information in this Qualification Specification is correct at the time of publishing but may be subject to change.

NCFE is a registered charity (Registered Charity No. 1034808) and a company limited by guarantee (Company No. 2896700).

**** To continue to improve our levels of customer service, telephone calls may be recorded for training and quality purposes.***

Appendix A: units

To simplify cross-referencing assessments and quality assurance, we have used a sequential numbering system in this document for each unit.

☆ Knowledge-only units are indicated by a star. If a unit is not marked with a star, it is a skills unit or contains a mix of knowledge and skills.

Mandatory units

Unit number	Regulated unit number	Unit title	Level	GLH
☆ Unit 01	A/651/1095	Cyber security concepts	3	45
Unit 02	D/651/1096	Cyber security threats, vulnerabilities and risks	3	54
Unit 03	F/651/1097	Risk and vulnerability assessment	3	54
Unit 04	H/651/1098	Incident response and disaster recovery	3	54
Unit 05	J/651/1099	Legislation and governance	3	54
Unit 06	T/651/1100	Cyber security measures	3	54
Unit 07	Y/651/1101	Professional development in cyber security	3	45

The units above may be available as stand-alone unit programmes. Please visit the NCFE website for further information.

Change history record

Version	Publication date	Description of change
v1.0	August 2025	First publication