

A large teal-colored rectangular box with a thin black border, containing the main title of the document.

# **Qualification specification**

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



**Qualification summary**

<b>Qualification title</b>	NCFE Level 3 Technical Occupational Entry in Cyber Security (Diploma)		
<b>Ofqual qualification number (QN)</b>	610/4004/6	<b>Aim reference</b>	61040046
<b>Guided learning hours (GLH)</b>	360	<b>Total qualification time (TQT)</b>	480
<b>Minimum age</b>	19		
<b>Qualification purpose</b>	<p>This qualification is designed to provide learners with the knowledge, skills and behaviours (KSBs) relevant to developing competence in cyber security.</p> <p>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.</p>		
<b>Grading</b>	Not yet achieved/pass/merit/distinction.		
<b>Assessment method</b>	Internally assessed and externally quality assured portfolio of evidence.		
<b>Occupational standards</b>	<p>This qualification is mapped against the following occupational standard:</p> <p>ST0865: Cyber Security Technician (Level 3) Version 1.0</p> <p>A mapping document is available on the qualification's page on the NCFE website.</p>		
<b>UCAS</b>	Please refer to the UCAS website for further details of points allocation and the most up-to-date information.		
<b>Regulation information</b>	This is a regulated qualification. The regulated number for this qualification is 610/4004/6.		
<b>Funding</b>	This qualification may be eligible for funding. For further guidance on funding, please contact your local funding provider.		

## Contents

<b>Qualification summary</b>	<b>2</b>
<b>Section 1: introduction</b>	<b>4</b>
Aims and objectives	4
Support handbook	4
Guidance for entry and registration	4
Achieving this qualification	4
Resource requirements	5
How the qualification is assessed	5
Internal assessment	6
Grading information	7
Grading internally assessed units	7
Awarding the final grade	7
<b>Section 2: unit content and assessment guidance</b>	<b>9</b>
Unit 01 Cyber security concepts (A/651/1095)	10
Unit 02 Cyber security threats, vulnerabilities and risks (D/651/1096)	15
Unit 03 Risk and vulnerability assessment (F/651/1097)	24
Unit 04 Incident response and disaster recovery (H/651/1098)	32
Unit 05 Legislation and governance (J/651/1099)	36
Unit 06 Cyber security measures (T/651/1100)	43
Unit 07 Professional development in cyber security (Y/651/1101)	50
Assessment strategies and principles	55
<b>Section 3: explanation of terms</b>	<b>56</b>
<b>Section 4: support</b>	<b>58</b>
Support materials	58
Other support materials	58
Reproduction of this document	58
<b>Contact us</b>	<b>59</b>
<b>Appendix A: units</b>	<b>60</b>

## 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.

If you are using this qualification specification for planning purposes, please make sure that you are using the most recent version.

## 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. The aim 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 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 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 **7** 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

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

## 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.

## 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 (IQA) 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).

All the evidence generated by the learner will be assessed against the standards expected of a level 3 learner for each LO.

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 internally assessed 7 units, which can be found within a separate document in the member's area of our 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 knowledge LOs for 7 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. Examples of suitable evidence for the portfolio for each unit are provided in section 2.

If a centre needs to create their own internal assessment tasks, there are 4 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 assessment criteria (AC)
- having a valid and engaging context or scenario
- including sufficient opportunities for stretch and challenge for higher attainers

### **External quality assurance (EQA)**

Summatively assessed and internally quality assured grades for completed units must be submitted via the Portal, prior to an external quality assurance (EQA) review taking place. Following the EQA review, the unit grades will either be accepted and banked by your external quality assurer 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.

## 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 AC within the units. Assessors must be confident that, as a minimum, all AC 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.

Once assessors are confident that all the pass descriptors have been met, they can move on to decide if the merit descriptors have been met. If the assessor is confident that all the merit descriptors have been met, they can decide if the distinction descriptors have been met. As the grading descriptors build up from the previous grade's criteria, the evidence must meet 100% of the grade's descriptors to be awarded that grade 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.

Centres must then submit each unit grade via the Portal. The grades submitted will be checked and confirmed through the EQA 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 GLH and a score based on the holistic grade. The overall grade achieved for each unit is converted to a uniform mark scale (UMS) score. The UMS score for each unit is then combined and converted into an overall qualification grade.

All of the AC needs 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 UMS scores for each unit. The total UMS will then be converted into a grade based on the following fixed thresholds:

	<b>Max</b>	<b>P</b>	<b>M</b>	<b>D</b>
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
29–35	D
17–28	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 Portal.

For further information on assessment, please refer to the user guide to the external quality assurance review report.

**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.

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.

DRAFT

**Unit 01 Cyber security concepts (A/651/1095)**



<b>Unit summary</b>			
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.			
<b>Assessment</b>			
This unit is internally assessed and externally quality assured.			
<b>Mandatory</b>	<b>Graded P/M/D</b>	<b>Level 3</b>	<b>45 GLH</b>

<b>Learning outcomes (LOs)</b> The learner will:	<b>Assessment criteria (AC)</b>	<b>Pass</b> The learner will be able to:	<b>Merit</b> The learner will be able to:	<b>Distinction</b> The learner will show evidence of:
1. Understand the key concepts within cyber security	1.1 The key concepts and importance of cyber security: <ul style="list-style-type: none"> <li>• CIA triad:                             <ul style="list-style-type: none"> <li>○ confidentiality</li> <li>○ integrity</li> <li>○ availability</li> </ul> </li> <li>• IAAA:                             <ul style="list-style-type: none"> <li>○ identification</li> <li>○ authentication</li> <li>○ authorisation</li> <li>○ accountability</li> </ul> </li> </ul>	Outline the concepts and importance 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. Examples are used to provide context alongside the application of core terminology.	Exploring the key concepts within cyber security in depth, demonstrating a clear understanding, with evidence of relevant research throughout.

<b>Learning outcomes (LOs)</b> The learner will:	<b>Assessment criteria (AC)</b>	<b>Pass</b> The learner will be able to:	<b>Merit</b> The learner will be able to:	<b>Distinction</b> The learner will show evidence of:
	1.2 The use of core terminology in cyber security: <ul style="list-style-type: none"> <li>• assurance</li> <li>• reliability</li> <li>• non-repudiation</li> <li>• access control</li> <li>• threat</li> <li>• vulnerability</li> <li>• risk</li> <li>• security breach</li> <li>• information security</li> <li>• attack vectors</li> <li>• attack surface</li> </ul>	Identify the use of core terminology in cyber security (as identified in AC1.2).		
	1.3 The role of information assurance and governance (IAG): <ul style="list-style-type: none"> <li>• to guide the development and improvement of policies and processes</li> <li>• to support the auditing of policies and processes</li> </ul>	Outline the role of IAG (as identified in AC1.3).	Define IAG and explain how it plays an important role in the development, improvement and auditing of policies and processes, ensuring legal and organisational compliance through the use of exemplars.	

<b>Learning outcomes (LOs)</b> The learner will:	<b>Assessment criteria (AC)</b>	<b>Pass</b> The learner will be able to:	<b>Merit</b> The learner will be able to:	<b>Distinction</b> The learner will show evidence of:
	<ul style="list-style-type: none"> <li>to provide confirmation of compliance (for example, with International Standards Organisation (ISO) standards)</li> </ul>			
2. Understand effective cyber security culture	2.1 The influence of organisational structures on cyber security culture: <ul style="list-style-type: none"> <li>stakeholders (for example, internal or external)</li> <li>organisational types (for example, public or private)</li> </ul>	Outline the influence of organisational structures on cyber security culture (as identified in AC2.1).	Discuss the importance of protecting the confidentiality of an organisation's information, using relevant examples, for a wide range of stakeholders, with consideration of different organisation types.	Providing an in-depth discussion of building and maintaining an effective cyber security culture, using relevant technical terminology with logical reasoning and evidence of relevant research throughout. Any recommendations made should be fully justified.
	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.		

<b>Learning outcomes (LOs)</b> The learner will:	<b>Assessment criteria (AC)</b>	<b>Pass</b> The learner will be able to:	<b>Merit</b> The learner will be able to:	<b>Distinction</b> The learner will show evidence of:
	2.3 The components and importance of an effective security culture	Outline the components and importance of an effective security culture.	Evidence should be supported through the use of working examples to help illustrate the importance of 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: <ul style="list-style-type: none"> <li>• hardware</li> <li>• software</li> <li>• operating systems (OSs)</li> <li>• network resources</li> </ul>	Outline the components of a secure infrastructure within an organisation (as identified in AC3.1).	Explore methods and techniques for securing infrastructure within an organisation with considerations of implementing cloud-based services and the benefits this offers.	Providing an in-depth understanding of secure infrastructure and cloud environments. Relevant examples should be used throughout.

<b>Learning outcomes (LOs)</b> The learner will:	<b>Assessment criteria (AC)</b>	<b>Pass</b> The learner will be able to:	<b>Merit</b> The learner will be able to:	<b>Distinction</b> The learner will show evidence of:
	3.2 The components of cloud environments: <ul style="list-style-type: none"> <li>• Infrastructure as a Service (IaaS)</li> <li>• Platform as a Service (PaaS)</li> <li>• Software as a Service (SaaS)</li> </ul>	Outline the components of cloud environments (as identified in AC3.2).		

DRAFT

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

<b>Unit summary</b>			
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.			
<b>Assessment</b>			
This unit is internally assessed and externally quality assured.			
<b>Mandatory</b>	<b>Graded P/M/D</b>	<b>Level 3</b>	<b>54 GLH</b>

<b>Learning outcomes (LOs)</b> The learner will:	<b>Assessment criteria (AC)</b>	<b>Pass</b> The learner will be able to:	<b>Merit</b> The learner will be able to:	<b>Distinction</b> 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.	A comprehensive understanding of cyber security threats and how to perform intelligence gathering through research-based activity. This provides clear evidence of an analysis of potential threats and reconnaissance techniques.
	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.	Explore threat actors in detail, discussing their motivation, the type of attack they may be	

<b>Learning outcomes (LOs)</b> The learner will:	<b>Assessment criteria (AC)</b>	<b>Pass</b> The learner will be able to:	<b>Merit</b> The learner will be able to:	<b>Distinction</b> The learner will show evidence of:
	1.4 Types of threats and the methods used to identify them (for example, social engineering, ransomware, zero-day, commodity threat)	Identify the types of threats and the methods used to identify them.	responsible for and the impact this could have on an organisation. Illustrative examples can be used to support the discussion.	
	1.5 The types and motivations of threat actors: <ul style="list-style-type: none"> <li>• nation state</li> <li>• script kiddies</li> <li>• cyber criminals</li> <li>• terrorist organisations</li> <li>• insiders</li> <li>• hacktivists</li> </ul>	Identify the types and motivations of threat actors (as identified in AC1.5).		
	1.6 The application of network reconnaissance techniques to identify threats: <ul style="list-style-type: none"> <li>• indicators of compromise (IOCs) from external threat</li> </ul>	Summarise the application of network reconnaissance techniques to identify threats (as identified in AC1.6).	Compare the range of network reconnaissance techniques identified, clearly explaining how these can be used to assist threat identification.	



<b>Learning outcomes (LOs)</b> The learner will:	<b>Assessment criteria (AC)</b>	<b>Pass</b> The learner will be able to:	<b>Merit</b> The learner will be able to:	<b>Distinction</b> The learner will show evidence of:
	intelligence sources <ul style="list-style-type: none"> <li>• use of tools to scan and analyse network traffic</li> <li>• monitoring:                             <ul style="list-style-type: none"> <li>○ unusual volume of network traffic</li> <li>○ repeated attempts to access systems</li> <li>○ alerts from end points</li> <li>○ abnormal user behaviour</li> <li>○ unexpected system changes</li> </ul> </li> </ul>			
	1.7 Perform routine threat intelligence gathering tasks using reliable sources	Demonstrate the ability to perform routine threat intelligence gathering tasks using reliable sources.		

<b>Learning outcomes (LOs)</b> The learner will:	<b>Assessment criteria (AC)</b>	<b>Pass</b> The learner will be able to:	<b>Merit</b> The learner will be able to:	<b>Distinction</b> The learner will show evidence of:
2. Understand suspicious activities and potential breaches	2.1 The characteristics of unusual security activity: <ul style="list-style-type: none"> <li>• suspicious user behaviour (for example, brute force attack)</li> <li>• suspicious device behaviour (for example, unusual network activity)</li> <li>• unauthorised system changes (for example, changes to network configuration)</li> <li>• malware activity (for example, IOCs)</li> </ul>	Outline the characteristics of unusual security activity (as identified in AC2.1).	Compare a range of unusual security activity clearly in relation to the category it falls into (as identified in AC2.1) and identify a procedure that can be used to train staff in the awareness of one of these.	Using relevant research to show a clear and comprehensive understanding of how to identify unusual security activity and training methods for raising awareness with stakeholders. This should be supported with the use of illustrative examples where appropriate.
	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.		

<b>Learning outcomes (LOs)</b> The learner will:	<b>Assessment criteria (AC)</b>	<b>Pass</b> The learner will be able to:	<b>Merit</b> The learner will be able to:	<b>Distinction</b> The learner will show evidence of:
	2.3 Develop information security training and awareness resources to support good cyber security practice	Demonstrate the ability to develop information security 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 the impact on security due to evolving risks and emerging technologies, clearly identifying how this could affect critical national infrastructure and control systems.	Using relevant research to show a comprehensive understanding of evolving cyber security issues. An in-depth explanation of critical national infrastructure and control systems is present.
	3.2 How evolving cyber security issues can impact critical national infrastructure and control systems: <ul style="list-style-type: none"> <li>• military and national defence (for example, leaking of classified information)</li> </ul>	Identify how evolving cyber security issues can impact critical national infrastructure and control systems (as identified in AC3.2).		

<b>Learning outcomes (LOs)</b> The learner will:	<b>Assessment criteria (AC)</b>	<b>Pass</b> The learner will be able to:	<b>Merit</b> The learner will be able to:	<b>Distinction</b> The learner will show evidence of:
	<ul style="list-style-type: none"> <li>• healthcare (for example, compromised confidentiality, ability to treat patients)</li> <li>• transport (for example, disruption to airlines, rail, smart motorways)</li> <li>• communication (for example, mass loss of service, interruptions to business and society)</li> <li>• utilities (for example, water and sanitation, energy sources)</li> <li>• supply chain (for example, production of food)</li> <li>• finance (for example,</li> </ul>			

<b>Learning outcomes (LOs)</b> The learner will:	<b>Assessment criteria (AC)</b>	<b>Pass</b> The learner will be able to:	<b>Merit</b> The learner will be able to:	<b>Distinction</b> The learner will show evidence of:
	disruption or failure of payment transactions) <ul style="list-style-type: none"> <li>operational technologies (OT) (for example, disruption to Supervisory Control and Data Acquisition (SCADA))</li> </ul>			
	3.3 The importance of the threat landscape and the associated risks to internet of things (IoT) devices (for example, privacy, compromising other devices on network, trustworthy brand)	Outline the importance of the threat landscape and the associated risks to IoT devices.		

<b>Learning outcomes (LOs)</b> The learner will:	<b>Assessment criteria (AC)</b>	<b>Pass</b> The learner will be able to:	<b>Merit</b> The learner will be able to:	<b>Distinction</b> The learner will show evidence of:
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: <ul style="list-style-type: none"> <li>• systems</li> <li>• services</li> <li>• devices</li> <li>• data storage</li> </ul>	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.	Discuss a range of methods that may be implemented for storing and managing digital information assets. The discussions should compare cloud-based storage options and the types of digital information assets (as identified in AC4.1).	Using relevant research to show a comprehensive understanding of digital information systems. This should contribute to a detailed discussion that incorporates a detailed comparison of local and cloud-based solutions, resulting in fully justified recommendations.
	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)	Identify the importance and application of maintaining a digital information asset inventory.	Describe the importance of maintaining an information asset inventory using relevant working examples where appropriate and explain how this is used to ensure the secure disposal of these assets.	
	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.		

<b>Learning outcomes (LOs)</b> The learner will:	<b>Assessment criteria (AC)</b>	<b>Pass</b> The learner will be able to:	<b>Merit</b> The learner will be able to:	<b>Distinction</b> The learner will show evidence of:
	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.		

DRAFT

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

<b>Unit summary</b>			
<p>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.</p>			
<b>Assessment</b>			
<p>This unit is internally assessed and externally quality assured.</p>			
<b>Mandatory</b>	<b>Graded P/M/D</b>	<b>Level 3</b>	<b>54 GLH</b>

<b>Learning outcomes (LOs)</b> The learner will:	<b>Assessment criteria (AC)</b>	<b>Pass</b> The learner will be able to:	<b>Merit</b> The learner will be able to:	<b>Distinction</b> 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: <ul style="list-style-type: none"> <li>• software misconfiguration (for example, authentication bypass, data loss)</li> <li>• broken access control and authentication (for example, unauthorised access)</li> </ul>	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, including support from working examples where appropriate.	Effectively explaining cyber security vulnerabilities with strong justifications, logical reasoning and demonstration of relevant research throughout.



<b>Learning outcomes (LOs)</b> The learner will:	<b>Assessment criteria (AC)</b>	<b>Pass</b> The learner will be able to:	<b>Merit</b> The learner will be able to:	<b>Distinction</b> The learner will show evidence of:
	<ul style="list-style-type: none"> <li>• sensitive data exposure (for example, reputational damage, fines)</li> <li>• injection vulnerabilities (for example, remote code execution, Denial of Service (DoS))</li> <li>• using components with known vulnerabilities (for example, software security weakness)</li> <li>• insufficient logging and monitoring (for example, unacknowledged persistent threat)</li> <li>• security misconfiguration (for example, lack of network</li> </ul>			

<b>Learning outcomes (LOs)</b> The learner will:	<b>Assessment criteria (AC)</b>	<b>Pass</b> The learner will be able to:	<b>Merit</b> The learner will be able to:	<b>Distinction</b> The learner will show evidence of:
	restrictions or anti-virus protection) <ul style="list-style-type: none"> <li>• incorrect cross-site validation (for example, session hijacking)</li> </ul>			
2. Understand and categorise cyber security risks for escalation	2.1 The process of risk management and risk assessment to categorise threats, vulnerabilities and risks: <ul style="list-style-type: none"> <li>• identification of the scope of the risk assessment</li> <li>• assessment of the risk using a scoring matrix (for example, probability versus impact)</li> <li>• categorisation of the risk rating (for example, apply a red, amber green (RAG) rating)</li> <li>• recording, responding or</li> </ul>	Outline of the process of risk management and risk assessment (as identified in AC2.1) to categorise threats, vulnerabilities and risks.	Describe how risk assessments are used to categorise vulnerabilities and threats through the application of a detailed and accurate risk matrix and risk register.	Using relevant research to thoroughly explore the categorisation of cyber security risks for escalation, demonstrating a comprehensive understanding. Any recommendations made include a well-rounded conclusion.

<b>Learning outcomes (LOs)</b> The learner will:	<b>Assessment criteria (AC)</b>	<b>Pass</b> The learner will be able to:	<b>Merit</b> The learner will be able to:	<b>Distinction</b> The learner will show evidence of:
	escalating as appropriate <ul style="list-style-type: none"> <li>• completion of a business impact analysis</li> </ul>			
	2.2 Identify and 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 to escalate information security events in accordance with relevant procedures and standards	Demonstrate the ability to identify when and how to escalate information security events in accordance with relevant procedures and standards.		

<b>Learning outcomes (LOs)</b> The learner will:	<b>Assessment criteria (AC)</b>	<b>Pass</b> The learner will be able to:	<b>Merit</b> The learner will be able to:	<b>Distinction</b> The learner will show evidence of:
3. Understand and evaluate vulnerability assessments	3.1 The considerations for a vulnerability assessment scope: <ul style="list-style-type: none"> <li>• networks</li> <li>• computers</li> <li>• servers</li> <li>• business units</li> <li>• applications</li> </ul>	Identify the considerations for a vulnerability assessment scope (as identified in AC3.1).	Examine a wide range of considerations that should be taken into account when identifying the scope of a vulnerability assessment, showing consideration for the tools and techniques used to evaluate this.	Clear research into evaluating vulnerability assessments, with justified recommendations, using appropriate technical terminology throughout. This should be supported through working examples where appropriate.
	3.2 The use of tools and techniques to evaluate vulnerability assessments: <ul style="list-style-type: none"> <li>• Common Vulnerabilities and Exposures (CVE)</li> <li>• Common Vulnerability Scoring System (CVSS)</li> </ul>	Identify the use of tools and techniques to evaluate vulnerability assessments (as identified in AC3.2).		
	3.3 Define the scope and objectives of vulnerability assessment	Demonstrate the ability to define the scope and objectives of a cyber security vulnerability assessment.		

<b>Learning outcomes (LOs)</b> The learner will:	<b>Assessment criteria (AC)</b>	<b>Pass</b> The learner will be able to:	<b>Merit</b> The learner will be able to:	<b>Distinction</b> The learner will show evidence of:
	3.4 How to make recommendations based on evidence from vulnerability assessment tools: <ul style="list-style-type: none"> <li>• severity of the vulnerability</li> <li>• potential impact and risk on business</li> <li>• availability of resources (for example, time, finances)</li> <li>• acceptance of risk</li> <li>• potential mitigations</li> <li>• scope of mitigation projects</li> </ul>	Identify how to make recommendations based on evidence from vulnerability assessment tools (as identified in AC3.4).	Describe how recommendations can be made based on the severity and impact of the vulnerability with consideration for potential mitigation techniques and resource constraints.	
	3.5 Evaluate the results of a cyber security vulnerability assessment	Demonstrate the ability to evaluate the results of a cyber security vulnerability assessment.		
4. Understand computer forensics	4.1 The concept of computer forensic principles:	Outline the concept of computer forensic principles (as identified in AC4.1).	Discuss the concepts of computer forensic principles with a focus on the key elements (as	Presenting clear research that supports a comprehensive understanding of computer

<b>Learning outcomes (LOs)</b> The learner will:	<b>Assessment criteria (AC)</b>	<b>Pass</b> The learner will be able to:	<b>Merit</b> The learner will be able to:	<b>Distinction</b> The learner will show evidence of:
	<ul style="list-style-type: none"> <li>• identification (for example, the evidence that is presented, where it is stored and how it can be accessed)</li> <li>• preservation (for example, isolating, securing and preserving evidence)</li> <li>• analysis (for example, evidence-based conclusions)</li> <li>• documentation (for example, retained in line with legal retention periods)</li> <li>• presentation (for example, evidence presented to law enforcement for further investigation)</li> </ul>		identified in AC4.1) to ensure that evidence is not compromised.	forensics, providing a foundation for any recommendations, justifications or conclusions that are made.

<b>Learning outcomes (LOs)</b> The learner will:	<b>Assessment criteria (AC)</b>	<b>Pass</b> The learner will be able to:	<b>Merit</b> The learner will be able to:	<b>Distinction</b> The learner will show evidence of:
	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.		

DRAFT

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

<b>Unit summary</b>			
<p>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.</p>			
<b>Assessment</b>			
<p>This unit is internally assessed and externally quality assured.</p>			
<b>Mandatory</b>	<b>Graded P/M/D</b>	<b>Level 3</b>	<b>54 GLH</b>

<b>Learning outcomes (LOs)</b> The learner will:	<b>Assessment criteria (AC)</b>	<b>Pass</b> The learner will be able to:	<b>Merit</b> The learner will be able to:	<b>Distinction</b> The learner will show evidence of:
1. Understand and create incident response documentation	1.1 The phases and application of the incident response lifecycle: <ul style="list-style-type: none"> <li>• preparation</li> <li>• detection and analysis</li> <li>• containment</li> <li>• eradication and recovery</li> <li>• post-event activity and lessons learned</li> </ul>	Outline the phases and the application of the incident response lifecycle (as identified in AC1.1).	Clearly explain the phases of the incident response lifecycle using examples, for each phase, to illustrate key information, highlighting where reporting plays an important part in the process.	An understanding of incident response documentation, through extensive research, that is used to formulate the identification of key information.



<b>Learning outcomes (LOs)</b> The learner will:	<b>Assessment criteria (AC)</b>	<b>Pass</b> The learner will be able to:	<b>Merit</b> The learner will be able to:	<b>Distinction</b> The learner will show evidence of:
	1.2 The application of exception reporting: <ul style="list-style-type: none"> <li>reporting of incidents (for example, breaches of information security policy)</li> </ul>	Outline the application of exception reporting.		
	1.3 The application of management reporting: <ul style="list-style-type: none"> <li>regular reporting (for example, recent events, threat landscape)</li> </ul>	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.		

<b>Learning outcomes (LOs)</b> The learner will:	<b>Assessment criteria (AC)</b>	<b>Pass</b> The learner will be able to:	<b>Merit</b> The learner will be able to:	<b>Distinction</b> The learner will show evidence of:
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 explain how this forms part of the chain of evidence.	A clear and well-articulated commentary, using relevant technical terminology. An understanding of creating cyber security incident information documentation is present.
	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, using illustrative examples, how monitoring systems are effectively used within an organisation as a method to check for security events.	Using monitoring systems, through research, to identify information security events, exploring in detail and using the findings to support recommendations.
	3.2 Monitor and report information security events to meet requirements	Demonstrate the ability to monitor and report information security events to meet requirements.		

<b>Learning outcomes (LOs)</b> The learner will:	<b>Assessment criteria (AC)</b>	<b>Pass</b> The learner will be able to:	<b>Merit</b> The learner will be able to:	<b>Distinction</b> The learner will show evidence of:
4. Understand disaster prevention and recovery	4.1 The use of disaster prevention and recovery methods to support continuity of service planning: <ul style="list-style-type: none"> <li>• disaster recovery plan (DRP)</li> <li>• business continuity plan (BCP)</li> </ul>	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, clearly explaining the purpose of DRPs and BCPs whilst considering how they differ in their approach, paying particular attention to backup and recovery.	Research that has been conducted into disaster prevention and recovery, which has been used throughout to support all findings.
	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)**

<b>Unit summary</b>			
<p>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.</p>			
<b>Assessment</b>			
This unit is internally assessed and externally quality assured.			
<b>Mandatory</b>	<b>Graded P/M/D</b>	<b>Level 3</b>	<b>54 GLH</b>

<b>Learning outcomes (LOs)</b> The learner will:	<b>Assessment criteria (AC)</b>	<b>Pass</b> The learner will be able to:	<b>Merit</b> The learner will be able to:	<b>Distinction</b> The learner will show evidence of:
1. Understand information security governance	1.1 The purpose of organisational security governance: <ul style="list-style-type: none"> <li>• provides a framework for managing compliance with legislation, standards, policies and processes</li> <li>• supports risk management</li> </ul>	Outline the purpose of organisational security governance (as identified in AC1.1).	Explain the purpose of organisational security governance through the use of illustrative examples.	A detailed understanding of information security governance through research.

<b>Learning outcomes (LOs)</b> The learner will:	<b>Assessment criteria (AC)</b>	<b>Pass</b> The learner will be able to:	<b>Merit</b> The learner will be able to:	<b>Distinction</b> The learner will show evidence of:
2. Understand and review cyber security policies	2.1 The value of an information security management system (ISMS) to support compliance with cyber security standards: <ul style="list-style-type: none"> <li>• people</li> <li>• processes</li> <li>• technology</li> </ul>	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 attention to compliance, policies and procedures.	Clear research, supporting a comprehensive understanding of cyber security policies. This should be supported through working examples where appropriate.
	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.		

<b>Learning outcomes (LOs)</b> The learner will:	<b>Assessment criteria (AC)</b>	<b>Pass</b> The learner will be able to:	<b>Merit</b> The learner will be able to:	<b>Distinction</b> The learner will show evidence of:
3. Understand knowledge of legislation relating to cyber security	3.1 The use of current legislation and standards to support cyber security: <ul style="list-style-type: none"> <li>• Data Protection Act 2018</li> <li>• Regulation of Investigatory Powers Act 2000</li> <li>• Human Rights Act 1998</li> <li>• Computer Misuse Act 1990</li> <li>• Freedom of Information Act 2000</li> <li>• Official Secrets Act 1989</li> <li>• Wireless Telegraphy Act 2006</li> <li>• Payment Card Industry Data Security Standard (PCI DSS)</li> </ul>	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 clearly identifying methods used to maintain currency of knowledge.	A detailed understanding of how to maintain knowledge of legislation relating to cyber security that is effectively explained with demonstration of relevant research throughout.

<b>Learning outcomes (LOs)</b> The learner will:	<b>Assessment criteria (AC)</b>	<b>Pass</b> The learner will be able to:	<b>Merit</b> The learner will be able to:	<b>Distinction</b> The learner will show evidence of:
	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: <ul style="list-style-type: none"> <li>• consent</li> <li>• contract</li> <li>• legal obligations</li> <li>• vital interests</li> <li>• public interest</li> <li>• legitimate interests</li> </ul>	Outline the ethical considerations when processing and storing data (as identified in AC4.1).	Explore codes of conduct in detail, highlighting how these support the ethical considerations.	An in-depth understanding of ethical considerations and codes of conduct, which is supported by research and the use of relevant examples where appropriate.

<b>Learning outcomes (LOs)</b> The learner will:	<b>Assessment criteria (AC)</b>	<b>Pass</b> The learner will be able to:	<b>Merit</b> The learner will be able to:	<b>Distinction</b> The learner will show evidence of:
	4.2 The attributes of ethical codes of conduct within cyber security: <ul style="list-style-type: none"> <li>• UK Cyber Security Council Code of Ethics</li> <li>• British Computer Society (BCS) Code of Conduct</li> <li>• Ethics for Incident Response and Security Teams (EthicsfIRST)</li> </ul>	Identify the attributes of ethical codes of conduct within cyber security (as identified in AC4.2).		
5. Understand cyber security policies and compliance	5.1 The purpose and application of common information security policies: <ul style="list-style-type: none"> <li>• acceptable use policy</li> <li>• incident management policy</li> <li>• bring your own device (BYOD) policy</li> </ul>	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 methods they will use to ensure compliance. The discussion should consider a range of techniques that can be used to monitor this.	Clear research into cyber security policies and compliance including justified recommendations supported by working examples.



<b>Learning outcomes (LOs)</b> The learner will:	<b>Assessment criteria (AC)</b>	<b>Pass</b> The learner will be able to:	<b>Merit</b> The learner will be able to:	<b>Distinction</b> The learner will show evidence of:
	<ul style="list-style-type: none"> <li>• access control policy</li> <li>• social media policy</li> <li>• password policy</li> <li>• patch management policy</li> <li>• anti-virus policy</li> <li>• information security policy</li> <li>• data classification and handling policy</li> <li>• IT asset disposal policy</li> </ul>			
	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.		

<b>Learning outcomes (LOs)</b> The learner will:	<b>Assessment criteria (AC)</b>	<b>Pass</b> The learner will be able to:	<b>Merit</b> The learner will be able to:	<b>Distinction</b> The learner will show evidence of:
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, explaining techniques used to ensure these are conducted in line with organisational procedures to ensure these are in an appropriate format.	A comprehensive understanding of cyber security auditing and the performance of compliance checks being explored in depth. There should be clear evidence showing the benefits of auditing and compliance to the organisation. This should be reinforced through research and any methods used should be justified.
	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)**

<b>Unit summary</b>			
<p>The learner will understand service desk delivery and 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.</p>			
<b>Assessment</b>			
<p>This unit is internally assessed and externally quality assured.</p>			
<b>Mandatory</b>	<b>Graded P/M/D</b>	<b>Level 3</b>	<b>54 GLH</b>

<b>Learning outcomes (LOs)</b> The learner will:	<b>Assessment criteria (AC)</b>	<b>Pass</b> The learner will be able to:	<b>Merit</b> The learner will be able to:	<b>Distinction</b> 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.	Discuss the function of service desk delivery, clearly identifying how these are used to resolve security related issues. The discussions should consider when and why a ticket may need escalating and the reason why this should be communicated in a clear and appropriate manner.	Research into service desk delivery, using this to support any recommendations made, concluding in clear justifications. Relevant examples should be included where appropriate.
	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.		
	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.		

<b>Learning outcomes (LOs)</b> The learner will:	<b>Assessment criteria (AC)</b>	<b>Pass</b> The learner will be able to:	<b>Merit</b> The learner will be able to:	<b>Distinction</b> The learner will show evidence of:
2. Understand, maintain and install cyber security controls	2.1 The types of cyber security controls: <ul style="list-style-type: none"> <li>• physical (for example, door access)</li> <li>• procedural (for example, acceptable use policy, vulnerability management policy, security incident response procedure)</li> <li>• technical (for example, firewalls, applications, user access control)</li> </ul>	Outline the types of cyber security controls (as identified in AC2.1).	Describe the different types of security controls, including examples for each, and discuss the measures and tools used by organisations and map these to the appropriate security control.	Understanding, maintaining and installing cyber security controls through thorough research and any conclusions are fully supported and justified.
	2.2 The application of common cyber security measures and tools: <ul style="list-style-type: none"> <li>• patching</li> <li>• software updates</li> <li>• access control</li> <li>• password management</li> </ul>	Outline the application of common cyber security measures and tools (as identified in AC2.2).		

<b>Learning outcomes (LOs)</b> The learner will:	<b>Assessment criteria (AC)</b>	<b>Pass</b> The learner will be able to:	<b>Merit</b> The learner will be able to:	<b>Distinction</b> The learner will show evidence of:
	<ul style="list-style-type: none"> <li>• firewalls</li> <li>• security incident and event management (SIEM) tools</li> <li>• protection tools:                             <ul style="list-style-type: none"> <li>○ anti-virus</li> <li>○ anti-malware</li> <li>○ anti-spam</li> </ul> </li> <li>• technical management and monitoring tools (for example, cloud security posture management (CSPM), cloud-native application protection platform (CNAPP))</li> </ul>			
	2.3 Maintain information security controls and measures	Demonstrate the ability to maintain information security controls and measures.		

<b>Learning outcomes (LOs)</b> The learner will:	<b>Assessment criteria (AC)</b>	<b>Pass</b> The learner will be able to:	<b>Merit</b> The learner will be able to:	<b>Distinction</b> The learner will show evidence of:
	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: <ul style="list-style-type: none"> <li>• eavesdropping of information</li> <li>• prevention of tampering of information to ensure integrity of data</li> <li>• assurance of authenticity of information</li> <li>• secure storage of sensitive data</li> </ul>	Outline the purpose of cryptography in cyber security (as identified in AC3.1).	Clearly explain the purpose and types of cryptography using appropriate examples and relevant technical terminology.	Conducting research on cryptography and digital certificates, clearly identifying their impact using examples, while incorporating accurate use of technical terminology.

<b>Learning outcomes (LOs)</b> The learner will:	<b>Assessment criteria (AC)</b>	<b>Pass</b> The learner will be able to:	<b>Merit</b> The learner will be able to:	<b>Distinction</b> The learner will show evidence of:
	3.2 Types of cryptographic techniques in cyber security: <ul style="list-style-type: none"> <li>• hashing</li> <li>• symmetric encryption (for example, Blowfish, Twofish)</li> <li>• asymmetric encryption (for example, Rivest-Shamir-Adleman (RSA), Diffie Hellman)</li> </ul>	Outline the types of cryptography in cyber security (as identified in AC3.2).		
	3.3 The use of digital certificates: <ul style="list-style-type: none"> <li>• to verify the identity of users</li> <li>• to verify servers</li> <li>• to sign data to prove authenticity</li> <li>• to secure communications in transit</li> </ul>	Outline the use of digital certificates (as identified in AC3.3).	Clearly explain the reasons for using digital certificates and discuss the tools used to manage these, using appropriate examples and technical terminology.	

<b>Learning outcomes (LOs)</b> The learner will:	<b>Assessment criteria (AC)</b>	<b>Pass</b> The learner will be able to:	<b>Merit</b> The learner will be able to:	<b>Distinction</b> The learner will show evidence of:
	3.4 The purpose of certificate management tools: <ul style="list-style-type: none"> <li>• generating certificate signing requests</li> <li>• signing new certificates</li> <li>• secure management of keys</li> <li>• tracking expired certificates</li> <li>• revoking compromised certificates</li> </ul>	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: <ul style="list-style-type: none"> <li>• authentication</li> <li>• authorisation and federation</li> </ul>	Outline the principles of identity and access management (as identified in AC4.1).	Discuss the importance of access rights, control and management, comparing the different types of access controls whilst	Research that supports their findings in relation to understanding and modifying access controls. This will provide a sound basis for the evidence and



<b>Learning outcomes (LOs)</b> The learner will:	<b>Assessment criteria (AC)</b>	<b>Pass</b> The learner will be able to:	<b>Merit</b> The learner will be able to:	<b>Distinction</b> The learner will show evidence of:
	4.2 The types and application of access control: <ul style="list-style-type: none"> <li>• mandatory access control (MAC)</li> <li>• discretionary access control (DAC)</li> <li>• attribute-based access control (ABAC)</li> <li>• role-based access control (RBAC)</li> <li>• rule-based access control (RuBAC)</li> </ul>	Outline the types and application of access control (as identified in AC4.2).	making recommendations for their use.	enhance a factual discussion.
	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)**

<b>Unit summary</b>			
<p>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.</p>			
<b>Assessment</b>			
<p>This unit is internally assessed and externally quality assured.</p>			
<b>Mandatory</b>	<b>Graded P/M/D</b>	<b>Level 3</b>	<b>45 GLH</b>

<b>Learning outcomes (LOs)</b> The learner will:	<b>Assessment criteria (AC)</b>	<b>Pass</b> The learner will be able to:	<b>Merit</b> The learner will be able to:	<b>Distinction</b> 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: <ul style="list-style-type: none"> <li>• customer issues and problems</li> <li>• business value</li> <li>• brand awareness</li> <li>• cultural/diversity awareness</li> </ul>	Outline the impact of digital transformation on cyber security occupations and within an overall business context (as identified in AC1.1).	Discuss ways in which the impact of digital transformation can be managed effectively, ensuring minimal disruption. This should be supported through examples where possible.	Research that supports findings in relation to understanding the impact of digital transformation. This will provide a sound basis for the evidence and enhance a factual discussion.

<b>Learning outcomes (LOs)</b> The learner will:	<b>Assessment criteria (AC)</b>	<b>Pass</b> The learner will be able to:	<b>Merit</b> The learner will be able to:	<b>Distinction</b> The learner will show evidence of:
	<ul style="list-style-type: none"> <li>• internal and external stakeholders:                             <ul style="list-style-type: none"> <li>○ user experience</li> <li>○ accessibility</li> <li>○ level of technical knowledge</li> </ul> </li> </ul>			
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 a range of current security occupations, identifying the impact regulatory requirements have on these and how these occupations may evolve. Where appropriate relevant examples should be included to support the response.	Exploring cyber security occupations in depth, demonstrating relevant research. This will provide a sound basis for the evidence and enhance a factual discussion on occupational evolution.
	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.		

<b>Learning outcomes (LOs)</b> The learner will:	<b>Assessment criteria (AC)</b>	<b>Pass</b> The learner will be able to:	<b>Merit</b> The learner will be able to:	<b>Distinction</b> The learner will show evidence of:
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, identifying the appropriateness of these in relation to CPD.	A comprehensive understanding of learning techniques and sources of knowledge through the use of research, which supports any comparisons and justified conclusions. Relevant examples should be included where appropriate.
	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.	Assess the reliability, validity and bias for a range of sources of knowledge used to support own professional development.	
	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.		

<b>Learning outcomes (LOs)</b> The learner will:	<b>Assessment criteria (AC)</b>	<b>Pass</b> The learner will be able to:	<b>Merit</b> The learner will be able to:	<b>Distinction</b> The learner will show evidence of:
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.	Clearly explain the benefits and limitations of implementing multidisciplinary teams using relevant working examples.	Research that supports a comprehensive understanding of multidisciplinary teams that provides a foundation for any recommendations, justifications or conclusions made.
	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.		
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.	Clearly explain the benefit of effective time management and stakeholder care when working to deadlines, demonstrating awareness of own practice.	Displaying reflective practice that is supported by research and relevant working examples where appropriate.
	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.		

<b>Learning outcomes (LOs)</b> The learner will:	<b>Assessment criteria (AC)</b>	<b>Pass</b> The learner will be able to:	<b>Merit</b> The learner will be able to:	<b>Distinction</b> The learner will show evidence of:
	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.		

DRAFT

## **Assessment strategies and principles relevant to this qualification**

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.

### **NCFE assessment strategy**

#### **Knowledge learning outcomes (LOs):**

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

#### **Skills learning outcomes (LOs):**

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

**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 terms are used in this qualification).

<b>Analyse</b>	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.
<b>Apply</b>	Explain how existing knowledge can be linked to new or different situations in practice.
<b>Clarify</b>	Explain the information in a clear, concise way.
<b>Classify</b>	Organise according to specific criteria.
<b>Collate</b>	Collect and present information arranged in sequential or logical order.
<b>Compare</b>	Examine the subjects in detail and consider the similarities and differences.
<b>Consider</b>	Think carefully and write about a problem, action or decision.
<b>Create</b>	Make or produce an artefact as required.
<b>Critically compare</b>	This is a development of 'compare' where the learner considers the positive aspects and limitations of the subject.
<b>Demonstrate</b>	Show an understanding by describing, explaining or illustrating using examples.
<b>Describe</b>	Write about the subject giving detailed information in a logical way.
<b>Develop (a plan/idea)</b>	Expand a plan or idea by adding more detail and/or depth of information.
<b>Diagnose</b>	Identify the cause based on valid evidence.
<b>Differentiate</b>	Identify the differences between 2 or more things.
<b>Discuss</b>	Write a detailed account giving a range of views or opinions.
<b>Distinguish</b>	Explain the difference between 2 or more items, resources or pieces of information.
<b>Draw conclusions</b>	Make a final decision or judgement based on reasons.
<b>Estimate</b>	Form an approximate opinion or judgement using previous knowledge or considering other information.



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

- evidence and grading tracker
- learning resources
- qualification factsheet

### 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.

### 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](mailto:customersupport@ncfe.org.uk)  
Website: [www.ncfe.org.uk](http://www.ncfe.org.uk)

**NCFE © Copyright 2023 All rights reserved worldwide.**

Draft 1.0 July 2023

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).


CACHE; Council for Awards in Care, Health and Education; and NNEB are registered trademarks owned by NCFE.

All the material in this publication is protected by copyright.

***\* 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 our website for further information.