

# Qualification Specification

**NCFE Level 4 Diploma: Cyber Security Engineer**  
**QN: 603/7748/3**



## Qualification summary

<b>Qualification title</b>	NCFE Level 4 Diploma: Cyber Security Engineer		
<b>Ofqual qualification number (QN)</b>	603/7748/3	<b>Aim reference</b>	60377483
<b>Guided learning hours (GLH)</b>	510	<b>Total qualification time (TQT)</b>	1200
<b>Credit value</b>	120		
<b>Minimum age</b>	18		
<b>Qualification purpose</b>	<p>This qualification is designed to give learners the knowledge and associated skills and behaviours required to work in a variety of roles in cyber security. It will also prepare learners to progress to further study and apprenticeships in this area.</p> <p>This qualification is designed for learners who want to upskill or retrain within the digital sector. It is also suitable for learners who want to further their studies in the digital sector. This higher technical qualification (HTQ) will give learners the skills, knowledge and behaviours to meet specific employer needs and industry requirements.</p>		
<b>Grading</b>	Pass/merit/distinction		
<b>Assessment method</b>	Internally assessed and externally quality assured portfolio of evidence, including task-based controlled assessments.		
<b>Work/industry placement experience</b>	Work/industry placement experience is not required.		
<b>Apprenticeship standards</b>	<p>This HTQ content has been aligned with the Cyber Security Technologist apprenticeship standard (cyber security engineer).</p> <p>This HTQ is designed to be delivered as a stand-alone qualification which is an alternative to the apprenticeship. It does not form part of an apprenticeship.</p>		
<b>Regulation information</b>	This is a regulated qualification. The regulated number for this qualification is 603/7748/3.		
<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>
Section 1: introduction	4
Aims and objectives	4
Support Handbook	4
Guidance for entry and registration	5
Achieving this qualification	5
Progression including job roles	5
Resource requirements	5
Real work environment (RWE) recommendation	6
How the qualification is assessed	6
Internal assessment	6
External quality assurance	7
Enquiries about results	7
Not yet achieved grade	7
Grading information	7
Grading internally assessed units	7
Awarding the final grade	8
Records of grades achieved for the NCFE Level 4 Diploma: Cyber Security Engineer (603/7748/3)	9
<b>Section 2: unit content and grading criteria</b>	<b>10</b>
Behavioural framework	10
Unit 01 Principles of cyber security (Y/651/0932)	12
Unit 02 Cyber security architecture (D/651/0934)	16
Unit 03 Legislation, policies and procedures in cyber security (F/651/0935)	21
Unit 04 Threat intelligence in cyber security (H/651/0936)	24
Unit 05 Risk assessment in cyber security (J/651/0937)	28
Unit 06 Cyber security management (K/651/0938)	30
Assessment strategies and principles relevant to this qualification	33
NCFE assessment strategy	33
<b>Section 3: explanation of terms</b>	<b>34</b>
<b>Section 4: support</b>	<b>36</b>
Support materials	36
Useful websites	36
Other support materials	36
Reproduction of this document	36
<b>Contact us</b>	<b>37</b>
<b>Appendix A: units</b>	<b>38</b>
Mandatory units	38

## 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.

A higher technical qualification (HTQ) is a prestigious, kite-marked qualification aimed at meeting employers' needs and increasing learner engagement in level 4 or 5 technical education. This HTQ content has been aligned with the Cyber Security Technologist (cyber security engineer) apprenticeship standard.

This qualification aims to:

- provide the knowledge, skills and behaviours that are needed to enter occupations across the country
- be understood and recognised as high-quality by employers and so have national labour market currency
- give learners confidence that those qualifications are recognised by employers and are perceived to be a credible, prestigious, and distinct pathway

## Aims and objectives

This qualification aims to:

- focus on the study of cyber security within the digital sector
- offer breadth and depth of study, incorporating a key core of knowledge
- provide opportunities to acquire a number of practical and technical skills

The objectives of this qualification are to provide learners with knowledge, skills and behaviours related to the following areas:

- principles of cyber security
- cyber security architecture
- legislation, policies and procedures in cyber security
- threat intelligence in cyber security
- risk assessment in cyber security
- cyber security management

## 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 for learners who want to begin or advance their career within cyber security. It is also suitable for learners who wish to progress to further study in this specialised area.

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 relevant level 3 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 must achieve 120 credits at a minimum of a pass in each of the 6 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. A partial certificate may be requested for learners who do not achieve the full qualification but have achieved at least one whole unit; partial achievement certificate fees can be found in the Fees and Pricing document on the NCFE website.

## Progression including job roles

Learners who achieve this qualification could progress to the following:

- employment:
  - cyber security engineer
  - cyber security consultant
  - cyber security architect
  - cyber security analyst
  - cyber security specialist
  - IT security technician
  - embedded engineer
- further education:
  - related apprenticeships
- higher education

## 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.

## Real work environment (RWE) recommendation

Where the assessment strategy for a qualification allows, it is essential that organisations wishing to operate a RWE do so in an environment that reflects a real work setting and replicates the key characteristics of the workplace in which the skill to be assessed is normally employed. This is often used to support simulation. Use of a RWE is not mandatory for this qualification.

## 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 4 Diploma: Cyber Security Engineer.

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.

All the evidence generated by the learner will be assessed against the standards expected of a level 4 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 units. 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 some LOs 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.

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 grading 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 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 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.

## Grading information

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

## Grading internally assessed units

The grading criteria for each unit have been included in the Qualification Specification. Grading criteria 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. NCFE has provided a grading criteria explanation of terms in the Qualification Specification to help you to make this judgement.

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 criteria 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 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.

All grading criteria 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

To achieve the qualification, learners must have achieved 120 credits at a minimum of a pass in each of the 6 mandatory units.

The calculation of the overall qualification grade is based on the learner's overall performance across all of the units. Learners are awarded their grade based on the points allocated for each grade, across all 120 credits. The table below shows the amount of points awarded for each credit, per unit.

Grade	Points per credit
Pass	1
Merit	3
Distinction	5

This means that if a learner gains a pass in a unit of 15 credits, they would receive 15 points. If they then gained a merit in a unit of 15 credits, they would receive 45 points. If they then gained distinction in their remaining units, totalling 90 credits, they would receive 450 points. This would give a total of 510 points, which would then be used to calculate the overall grade, using the table below.

The table below shows the overall total points required for each of the grade boundaries:

Grade	Points boundaries
Not yet achieved	0 to 119
Pass	120 to 299
Merit	300 to 499
Distinction	500+

The final grade for the qualification is based on a structure of not yet achieved, pass, merit or 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 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.**



**Records of grades achieved for the NCFE Level 4 Diploma: Cyber Security Engineer (603/7748/3)**

Grades achieved			Distinction		Merit		Pass		Points/grade
Unit number	Unit title	Credits per unit	Points per credit	Points	Points per credit	Points	Points per credit	Points	
Y/651/0932	Principles of cyber security	20	5	100	3	60	1	20	
D/651/0934	Cyber security architecture	30	5	150	3	90	1	30	
F/651/0935	Legislation, policies and procedures in cyber security	10	5	50	3	30	1	10	
H/651/0936	Threat intelligence in cyber security	30	5	150	3	90	1	30	
J/651/0937	Risk assessment in cyber security	15	5	75	3	45	1	15	
K/651/0938	Cyber security management	15	5	75	3	45	1	15	
							<b>Total points</b>		

## Section 2: unit content and grading criteria

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

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. Centres can select suitable assessment methods. A range of assessment methods should be used to holistically assess a range of criteria where possible. Centres should use the requirements of the unit, and the grading criteria to determine suitable assessment methods that are relevant to the requirements of the industry. For approval of methods of internal assessment other than portfolio building, please contact your external quality assurer (EQA).

Sample assignment briefs and tasks have been created for some of the LOs within the units. These sample assignment briefs and tasks are not mandatory. Centres may adapt these briefs and/or tasks to suit the needs of their learners to help build up their evidence, or they can develop their own. The sample assignment briefs, and tasks have been designed to demonstrate coverage of a selection of the knowledge and/or skills LOs and provide opportunities for stretch and challenge.

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.

### Behavioural framework

Embedded within higher technical qualifications (HTQs) is the opportunity for learners to develop behaviours relevant to their chosen discipline, in line with the qualification's knowledge and skills.

The following table identifies opportunities to demonstrate the behaviours – embedded within the knowledge and skills – that will be assessed as part of this HTQ. Learners may also naturally demonstrate these behaviours elsewhere, beyond the listing below. All listed behaviours are subject to assessment.

- B1: Logical – applies logical thinking, for example, uses clear and valid reasoning when making decisions related to undertaking the work instructions
- B2: Analytical – working with data effectively to see patterns, trends and draw meaningful conclusions
- B3: Works independently and takes responsibility. For example, works diligently regardless of how much they are being supervised, and stays motivated and committed when facing challenges
- B4: Shows initiative, being resourceful when faced with a problem and taking responsibility for solving problems within their own remit
- B5: Thorough and organised. For example, uses their time effectively to complete work to schedule and takes responsibility for managing their own work load and time
- B6: Works effectively with a wide range of people in different roles, internally and externally, with a regard to inclusion and diversity policy
- B7: Communicates effectively in a wide variety of situations for example contributing effectively to meetings and presenting complex information to technical and non-technical audiences
- B8: Maintains a productive, professional and secure working environment
- B9: Creative – taking a variety of perspectives, taking account of unpredictable adversary and threat behaviours and approaches, bring novel and unexpected solutions to address cyber security challenges
- B10: Problem solving – identifies issues quickly, solves complex problems and applies appropriate solutions. Dedicated to finding the true root cause of any problem and find solutions that prevent recurrence

	Behaviours									
Unit	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10
1: Principles of cyber security	N/A	N/A	LO3	LO3	LO3	LO3	LO3	LO3	LO3	LO3
2: Cyber security architecture	LO2 LO3	N/A	LO1 LO3	LO1 LO2 LO3	LO1 LO2 LO3	N/A	N/A	LO1 LO2 LO3	LO1 LO2	LO1 LO2 LO3
3: Legislation, policies and procedures in cyber security	N/A	N/A	LO3	N/A	LO3	LO3	LO3	LO3	N/A	N/A
4: Threat intelligence in cyber security	LO1 LO2 LO3	LO1 LO3	LO1 LO3	LO1 LO2 LO3	LO1 LO2 LO3	LO1 LO3	LO1 LO3	LO1 LO2 LO3	LO2 LO3	LO1 LO2 LO3
5: Risk assessment in cyber security	LO2	N/A	LO2	LO2	LO2	LO2	LO2	LO2	LO2	LO2
6: Cyber security management	LO1	LO1	N/A	LO1	LO1	LO1	LO1	LO1	LO1	LO1

## Unit 01 Principles of cyber security (Y/651/0932)

Unit summary				
This unit explores the principles of cyber security and the need to guard sensitive data and shield digital assets from constant threats.				
Assessment				
Internally assessed unit				
<b>Mandatory</b>	<b>Graded P/M/D</b>	<b>Level 4</b>	<b>20 credits</b>	<b>105 GLH</b>

Learning outcomes (LOs)	Mandatory teaching content
1. Examine principles of cyber security within organisations and society	<p><b>Knowledge:</b></p> <p>Principles of cyber security:</p> <ul style="list-style-type: none"> <li>• CIA Triad: <ul style="list-style-type: none"> <li>○ confidentiality, integrity and availability</li> </ul> </li> <li>• IAAA: <ul style="list-style-type: none"> <li>○ identity, authentication, authorisation and audit</li> </ul> </li> <li>• non-repudiation</li> </ul> <p>Roles within organisation and society:</p> <ul style="list-style-type: none"> <li>• organisational and societal cyber defense</li> <li>• fortifying systems against threats</li> <li>• maintaining trust and privacy</li> </ul>
2. Explore factors that contribute to security functionality in cyber security	<p><b>Knowledge:</b></p> <p>Architecture frameworks in the planning and implementation of security architecture:</p> <ul style="list-style-type: none"> <li>• The Open Group Architecture Framework (TOGAF)</li> <li>• Sherwood applied business security architecture (SABSA)</li> <li>• open security architecture (OSA)</li> <li>• cloud security architecture (CSA)</li> <li>• enterprise information security architecture (EISA)</li> </ul> <p>Use of architecture diagrams:</p> <ul style="list-style-type: none"> <li>• network topology diagram</li> <li>• block definition diagram (BDD)</li> <li>• data flow diagram (DFD)</li> <li>• entity relationship diagrams (ERD)</li> </ul> <p>Use of cyber security technology components:</p> <ul style="list-style-type: none"> <li>• firewalls (for example, packet-filtering, proxy firewalls)</li> <li>• unified threat management (UTM)</li> </ul>

Learning outcomes (LOs)	Mandatory teaching content
	<ul style="list-style-type: none"> <li>• intrusion prevention system (IPS) and intrusion detection system (IDS)</li> <li>• access management (for example, multi-factor authentication (MFA))</li> <li>• secure communication (for example, secure sockets layer/transport layer security (SSL/TLS))</li> <li>• forward and reverse proxies</li> <li>• email filtering</li> <li>• end point protection (for example, antivirus/antimalware)</li> <li>• hardware security modules (HSM) and devices</li> </ul> <p>Application of methods to achieve assurance:</p> <ul style="list-style-type: none"> <li>• testing (for example, penetration testing)</li> <li>• vulnerability management</li> <li>• breach and attack simulation (BAS)</li> <li>• Mitre ATT&amp;CK framework</li> </ul>
<p>3. Apply programming and scripting languages to design or end user requirements</p>	<p><b>Knowledge:</b></p> <p>Types of programming and scripting languages:</p> <ul style="list-style-type: none"> <li>• programming:             <ul style="list-style-type: none"> <li>○ C#</li> <li>○ C++</li> <li>○ Java</li> </ul> </li> <li>• scripting:             <ul style="list-style-type: none"> <li>○ PowerShell</li> <li>○ Python</li> <li>○ JavaScript</li> <li>○ PHP</li> <li>○ SQL</li> </ul> </li> </ul> <p>Use cases for programming and scripting:</p> <ul style="list-style-type: none"> <li>• application development</li> <li>• automation</li> <li>• web pages</li> <li>• databases</li> <li>• attack simulation</li> </ul> <p>Common coding standards and approaches:</p> <ul style="list-style-type: none"> <li>• understandable variables</li> <li>• documented code</li> <li>• input validations</li> <li>• error handling</li> <li>• version control</li> </ul>

Learning outcomes (LOs)	Mandatory teaching content
	<ul style="list-style-type: none"> <li>• formatting</li> <li>• indentation</li> <li>• naming conventions</li> <li>• commenting</li> <li>• use of whitespace</li> </ul> <p>Employers and end user requirements:</p> <ul style="list-style-type: none"> <li>• web development</li> <li>• automation</li> <li>• mobile applications</li> <li>• interactive dashboards</li> <li>• customised CRM software</li> <li>• user stories</li> <li>• requirements gathering</li> </ul> <p><b>Skills:</b></p> <p>Write program code or scripts taking into account employer/end user requirements</p>

DRAFT

**Grading criteria**

<b>Learning outcomes (LOs)</b>	<b>Pass</b>	<b>Merit</b>	<b>Distinction</b>
<b>LO1:</b> Examine principles of cyber security within organisations and society	<b>P1:</b> Describe the role of cyber security principles within organisations and society	<b>M1:</b> Explain the principles of cyber security and principles within organisations and the wider society	<b>D1:</b> Justify the use of cyber security principles and technology components within organisations and the wider society
<b>LO2:</b> Explore factors that contribute to security functionality in cyber security	<b>P2:</b> Outline impact of cyber security technology components  <b>P3:</b> Describe security assurance methods and their application in meeting requirements	<b>M2:</b> Explain the purpose and application of components and frameworks	
<b>LO3:</b> Apply programming and scripting languages to design or end user requirements	<b>P4:</b> Produce a program code or script taking into account end user requirements	<b>M3:</b> Assess the suitability of the program code or script produced	<b>D2:</b> Evaluate the suitability of their program code or script in terms of suitability for the end user, making recommendations of suggested improvements
	<b>P5:</b> Explain variations when producing clean and maintainable code		

## Unit 02 Cyber security architecture (D/651/0934)

Unit summary				
This unit delves into the intricate realm of safeguarding digital landscapes through a comprehensive exploration of fundamental principles and practical applications. This unit empowers learners to reinforce their understanding of network principles, digital system components, operating system security and cryptography, all essential pillars in the domain of cyber security architecture.				
Assessment				
Internally assessed unit				
<b>Mandatory</b>	<b>Graded P/M/D</b>	<b>Level 4</b>	<b>30 credits</b>	<b>120 GLH</b>

Learning outcomes (LOs)	Mandatory teaching content
1. Explore networking model and protocols	<p><b>Knowledge:</b></p> <p>OSI and TCP/IP models and their comparative structures</p> <p>Characteristics of TCP/IP model:</p> <ul style="list-style-type: none"> <li>• network protocols:                             <ul style="list-style-type: none"> <li>○ User Datagram Protocol (UDP)</li> <li>○ Transmission Control Protocol (TCP)</li> </ul> </li> <li>• addressing and naming:                             <ul style="list-style-type: none"> <li>○ IPv4</li> <li>○ IPv6</li> <li>○ domain name system (DNS)</li> <li>○ dynamic host configuration protocol (DHCP)</li> <li>○ subnet and subnet masks</li> </ul> </li> </ul> <p>The relationship between applications, protocols, ports, services and devices within the OSI and TCP/IP model</p> <p>Types of routing protocol:</p> <ul style="list-style-type: none"> <li>• dynamic</li> <li>• static</li> </ul> <p>Network issues and common failure modes:</p> <ul style="list-style-type: none"> <li>• congestion</li> <li>• hardware failures</li> <li>• software bugs</li> <li>• physical damage to infrastructure</li> </ul> <p>The effects of network issues and common failure modes on a network's performance</p> <p>Approaches to error control within networks:</p>



Learning outcomes (LOs)	Mandatory teaching content
	<ul style="list-style-type: none"> <li>• redundancy</li> <li>• automatic retransmissions</li> <li>• error detection codes</li> <li>• firewalls and intrusion detection systems</li> <li>• back up and disaster recovery plans</li> </ul> <p>Types of virtual networks:</p> <ul style="list-style-type: none"> <li>• virtual private network (VPN)</li> <li>• virtual local area network (VLAN)</li> <li>• virtual extensible local area network (VXLAN)</li> </ul> <p>Securing connections between virtual networks and physical networks</p> <p><b>Skills:</b></p> <p>Design, build and test a network to meet requirements:</p> <ul style="list-style-type: none"> <li>• multiple subnets</li> <li>• static and dynamic routes</li> </ul>
<p>2. Apply the characteristics of digital system components, implementing security controls</p>	<p><b>Knowledge:</b></p> <p>Function and features of digital system components:</p> <ul style="list-style-type: none"> <li>• switch</li> <li>• router</li> <li>• firewall</li> <li>• next-generation firewall (NGFW)</li> <li>• wireless access point</li> <li>• server</li> <li>• client</li> </ul> <p>Vulnerabilities and mitigation techniques within digital systems:</p> <ul style="list-style-type: none"> <li>• network</li> <li>• cloud</li> <li>• operating system (OS)</li> <li>• software</li> </ul> <p><b>Skills:</b></p> <p>Design and build a system that meets the requirements of a security case, selecting, configuring and deploying hardware and software components</p> <p>Test the implemented security controls and record outcomes</p>

Learning outcomes (LOs)	Mandatory teaching content
3. Apply the concepts of cryptography	<p><b>Knowledge:</b></p> <p>Use of centralised key management systems</p> <p>The use of centralised key management systems to provide a single point encryption solution for organisations (for example, monitoring expiration dates of keys)</p> <p>Uses of cryptography (for example, time stamping, blockchain)</p> <p>Methods of cryptography:</p> <ul style="list-style-type: none"> <li>• symmetric encryption: <ul style="list-style-type: none"> <li>○ single key</li> </ul> </li> <li>• asymmetric encryption: <ul style="list-style-type: none"> <li>○ multiple keys</li> </ul> </li> <li>• hashing</li> </ul> <p>The influence of international export controls on cryptography</p> <p>Application of digital certificates</p> <p>Phases of the encryption key management lifecycle:</p> <ul style="list-style-type: none"> <li>• generation</li> <li>• distribution</li> <li>• rotation</li> <li>• storage</li> <li>• archival</li> <li>• destruction</li> </ul> <p><b>Skills:</b></p> <p>Design a system that employs encryption techniques to meet security objectives</p> <p>Develop and implement a plan for managing and storing encryption keys to meet requirements</p>

## Grading criteria

Learning outcomes (LOs)	Pass	Merit	Distinction
<b>LO1:</b> Explore networking model and protocols	<b>P1:</b> Describe the structure and layers of the OSI and TCP/IP models including core TCP/IP protocols and IP addressing	<b>M1:</b> Illustrate the relationship between applications, protocols, ports, services and devices within the OSI and TCP/IP	<b>D1:</b> Evaluate the suitability of different networking protocols and models for specific scenarios, taking security considerations into account
	<b>P2:</b> Outline common network issues and error control		
	<b>P3:</b> Design and implement a network with multiple subnets and routing		
<b>LO2:</b> Apply the characteristics of digital system components, implementing security controls	<b>P4:</b> Identify common digital system components (switches, routers, firewalls, servers) and their functions	<b>M2:</b> Propose a comprehensive security plan for a complex digital system	<b>D2:</b> Justify the selection of components and controls in a security plan
	<b>P5:</b> Design and test a system that incorporates appropriate security controls based on a given security case study	<b>M3:</b> Outline mitigation techniques for identified vulnerabilities	
<b>LO3:</b> Apply the concepts of cryptography	<b>P6:</b> Describe the principles of symmetric and asymmetric encryption and hashing	<b>M4:</b> Differentiate between various encryption algorithms in terms of strength and use cases	<b>D3:</b> Analyse security trade-offs between different encryption algorithms and key management approaches
	<b>P7:</b> Design a basic encryption scheme to protect data based on specific security requirements		

	<p><b>P8:</b> Develop a secure key management plan, including rotation, storage and archival strategies, addressing potential vulnerabilities</p>		
--	---	--	--

DRAFT

## Unit 03 Legislation, policies and procedures in cyber security (F/651/0935)

Unit summary				
This unit offers an essential exploration into the intricate web of legal frameworks, standards and management practices that form the foundation of effective cyber security governance. This unit equips learners with a comprehensive understanding of the critical relationship between regulatory compliance, policies, and operational procedures in safeguarding digital environments.				
Assessment				
Internally assessed unit				
<b>Mandatory</b>	<b>Graded P/M/D</b>	<b>Level 4</b>	<b>10 credits</b>	<b>45 GLH</b>

Learning outcomes (LOs)	Mandatory teaching content
1. Explore the fundamentals of common legislation and standards applicable to cyber security	<p><b>Knowledge:</b></p> <p>The features and application of legislation, regulations and standards:</p> <ul style="list-style-type: none"> <li>• Data Protection Act (DPA) 2018 – UK General Data Protection Regulation (GDPR) including Article 32</li> <li>• Computer Misuse Act 1990</li> <li>• Copyright, Designs and Patents Act 1988</li> <li>• Intelligence Services Act 1994</li> <li>• Regulation of Investigatory Powers Act (RIPA) 2000</li> <li>• ISO 27001</li> <li>• National Cyber Security Centre (NCSC): <ul style="list-style-type: none"> <li>○ Cyber Essentials and Cyber Essentials Plus</li> <li>○ Cyber Assessment Framework (CAF)</li> </ul> </li> <li>• National Institute of Standards and Technology (NIST)</li> </ul> <p>Ethical principles and codes of good practice in cyber security (for example, UK Cyber Security Council Code of Ethics, NCSC Code of Conduct)</p>

Learning outcomes (LOs)	Mandatory teaching content
2. Examine common factors of security management	<p><b>Knowledge:</b></p> <p>Security management factors:</p> <ul style="list-style-type: none"> <li>• governance</li> <li>• compliance with standards (for example, ISO 27001) and guidelines (service level agreements (SLA))</li> <li>• compliance with relevant organisational policies and procedures (for example, identity and access management (IAM))</li> <li>• roles and responsibilities within an organisational structure</li> </ul> <p>The relationship between security management and the desired security outcomes:</p> <ul style="list-style-type: none"> <li>• clear security strategy</li> <li>• accountability and oversight</li> <li>• defined security roles</li> <li>• competent workforce</li> <li>• cross-functional collaboration</li> <li>• adherence to industry standards</li> <li>• incident response readiness</li> <li>• risk, asset and chain management</li> <li>• data and system security</li> <li>• staff awareness and education</li> </ul>
3. Apply the fundamentals of IT service management (ITSM)	<p><b>Knowledge:</b></p> <p>IT service management (ITSM):</p> <ul style="list-style-type: none"> <li>• objectives (for example, enhance vulnerability management, data and system security)</li> <li>• benefits (for example, improved risk management, enhanced user satisfaction)</li> </ul> <p>The application of information technology infrastructure library (ITIL) to support the implementation of ITSM</p> <p>The relationship between ITSM attributes and their importance to inform successful ITSM:</p> <ul style="list-style-type: none"> <li>• people</li> <li>• products</li> <li>• partners</li> <li>• processes</li> <li>• assets and their relationships</li> </ul>

Learning outcomes (LOs)	Mandatory teaching content
	<p><b>Skills:</b></p> <p>Apply and comply with organisational policies, standards and SLA targets associated with security management</p>

### Grading criteria

Learning outcomes (LOs)	Pass	Merit	Distinction
<p><b>LO1:</b> Explore the fundamentals of common legislation and standards applicable to cyber security</p>	<p><b>P1:</b> Summarise the application of legislation, regulations and standards on effective security practices</p>	<p><b>M1:</b> Suggest improvements to policies for an example company</p>	<p><b>D1:</b> Justify improvements against cyber security regulations and standards</p>
	<p><b>P2:</b> Explain the importance of codes of good practice to an organisation</p>		
<p><b>LO2:</b> Examine common factors of security management</p>	<p><b>P3:</b> Explain the links between factors of security management and desired security outcomes</p>	<p><b>M2:</b> Discuss the impact and influence of factors on security management</p>	<p><b>D2:</b> Evaluate how factors and standards are used to meet desired outcomes in a security management framework</p>
<p><b>LO3:</b> Apply the fundamentals of IT service management (ITSM)</p>	<p><b>P4:</b> Create an ITSM plan for an organisation</p>	<p><b>M3:</b> Explain how the plan complies with policies, standards and SLA targets</p>	

## Unit 04 Threat intelligence in cyber security (H/651/0936)

Unit summary				
This unit delves into the dynamic realm of identifying, analysing and countering cyber threats through a comprehensive exploration of the threat intelligence lifecycle. This unit empowers learners with the knowledge and skills to proactively defend digital ecosystems by understanding, anticipating and mitigating a wide array of cyber threats.				
Assessment				
Internally assessed unit				
<b>Mandatory</b>	<b>Graded P/M/D</b>	<b>Level 4</b>	<b>30 credits</b>	<b>120 GLH</b>

Learning outcomes (LOs)	Mandatory teaching content
1. Explore common cyber security threats and attack techniques	<p><b>Knowledge:</b></p> <p>Common threat actors:</p> <ul style="list-style-type: none"> <li>hackers/hacktivists and script kiddies</li> <li>insiders</li> <li>nation state</li> <li>cyber criminals</li> <li>terrorist organisations</li> <li>competitors</li> <li>thrill seekers</li> </ul> <p>Motivations and opportunities for threat actors to carry out cyber-attacks (for example, financial gain, disruption, mismanaged third party services, political changes)</p> <p>Common system-focused attack techniques:</p> <ul style="list-style-type: none"> <li>denial of service (DoS) and distributed denial of service (DDoS)</li> <li>SQL injection and cross-site scripting (XSS)</li> <li>spyware and malware</li> <li>zero-day exploit</li> <li>on-path attacks</li> <li>ransomware</li> <li>remote access trojan (RAT)</li> <li>escalating privileges</li> </ul> <p>Common human-focused attack techniques:</p> <ul style="list-style-type: none"> <li>social engineering (for example, phishing, spear phishing)</li> <li>malicious insider attack</li> <li>non-malicious insider attack</li> </ul> <p>How attack techniques combine with motive and opportunity to become a threat</p>



Learning outcomes (LOs)	Mandatory teaching content
	<p><b>Skills:</b></p> <p>Analyse security threats and hazards using a range of external sources (for example, NCSC)</p> <p>Evaluate the potential impact of threats or hazards on business operations</p> <p>Source and analyse security case information including what threats, vulnerability or risks have been mitigated</p>
<p>2. Examine vulnerabilities and mitigations</p>	<p><b>Knowledge:</b></p> <p>Monitoring tools for vulnerability identification and assurance:</p> <ul style="list-style-type: none"> <li>• third party services</li> <li>• sources of internal and external knowledge and intelligence sharing:                             <ul style="list-style-type: none"> <li>○ log files</li> <li>○ Open Web Application Security Project (OWASP)</li> <li>○ The Cyber Security Body Of Knowledge (CyBOK)</li> <li>○ open-source intelligence (OSINT)</li> </ul> </li> <li>• alerts from technologies</li> <li>• WiFi traffic analysis</li> <li>• penetration testing</li> <li>• end user notification</li> <li>• network protocol analyser</li> <li>• dark web monitoring</li> <li>• security information and event management (SIEM) tools</li> <li>• configurations of tools</li> </ul> <p>The types, stages and application of penetration testing approaches</p> <p>Technical control methods to defend and mitigate vulnerabilities and risks:</p> <ul style="list-style-type: none"> <li>• firewalls</li> <li>• message parsing and validation</li> <li>• secure configuration</li> <li>• encryption</li> <li>• patch management</li> <li>• antivirus software</li> <li>• back-ups</li> <li>• traffic filtering</li> <li>• least permissions and access</li> <li>• privileged access management (PAM)</li> <li>• intrusion prevention system (IPS)</li> <li>• intrusion detection system (IDS)</li> <li>• multiprotocol label switching (MPLS)</li> <li>• multi-factor authentication (MFA)</li> </ul>

Learning outcomes (LOs)	Mandatory teaching content
	<p><b>Skills:</b></p> <p>Research and analyse information of common attack methods using a range of internal and external intelligence sharing initiatives</p> <p>Configure monitoring tools to identify threats and vulnerabilities based on intelligence</p> <p>Discover system vulnerabilities and use monitoring tools and technical control methods to actively prevent security breaches</p>
<p>3. Analyse the horizon of cyber security trends</p>	<p><b>Knowledge:</b></p> <p>The significance and value of identified cyber security trends through threat trend analysis</p> <p>Value of using common recognised sources of threat intelligence and vulnerabilities to support horizon scanning and the risk of acting upon incorrect threat intelligence</p> <p>Use of strategies to respond to emerging attack techniques (for example, breach attack simulation (BAS), incident response planning)</p> <p>The threat intelligence lifecycle:</p> <ul style="list-style-type: none"> <li>• planning and direction</li> <li>• collection</li> <li>• processing</li> <li>• analysis and production</li> <li>• dissemination and feedback</li> </ul> <p><b>Skills:</b></p> <p>Analyse existing cyber security approaches and recommend improvements, taking into consideration:</p> <ul style="list-style-type: none"> <li>• existing employer/end user approaches</li> <li>• threat trends</li> <li>• future potential threats</li> </ul>

## Grading criteria

Learning outcomes (LOs)	Pass	Merit	Distinction
<b>LO1:</b> Explore common cyber security threats and attack techniques	<b>P1:</b> Identify common threat actors, their motivations, and describes system-focused and human-focused attack techniques	<b>M1:</b> Explains the relationship between threat actor motivations, attack methods, and system vulnerabilities	<b>D1:</b> Critically evaluate the relative risks posed by different threat actors to a specific organisation
	<b>P2:</b> Explain security threats using external sources and evaluate their potential impact on business operations	<b>M2:</b> Analyse security case studies to evaluate the impact of threats on business operations, considering multiple factors	<b>D2:</b> Propose specific mitigation strategies tailored to counter both system-focused and human-focused attack techniques
<b>LO2:</b> Examine vulnerabilities and mitigations	<b>P3:</b> Identify various vulnerability monitoring tools and technical control methods, describing their purposes	<b>M3:</b> Explain how different monitoring tools and technical controls are used to identify and mitigate specific vulnerabilities	<b>D3:</b> Evaluate different monitoring tools and technical controls for a specific security context
	<b>P4:</b> Configure basic monitoring tools to proactively identify threats and vulnerabilities	<b>M4:</b> Analyse collected intelligence to optimise the configuration of monitoring tools for maximum effectiveness	<b>D4:</b> Justify the selection of controls based on identified vulnerabilities, and actively mitigate identified threats
<b>LO3:</b> Analyse the horizon of cyber security trends	<b>P5:</b> Describe the stages of the threat intelligence lifecycle, identifying reliable threat intelligence sources	<b>M5:</b> Analyse emerging attack techniques, recommending improvements to existing cyber security approaches based on trends	<b>D5:</b> Assess the potential impact of inaccurate information, and propose strategies for validation
	<b>P6:</b> Explain basic threat trend information to identify potential risks relevant to an organisation		

## Unit 05 Risk assessment in cyber security (J/651/0937)

Unit summary				
This unit provides a comprehensive exploration of the fundamental components of risk management as applied to the dynamic field of cyber security. This unit empowers learners with the knowledge and tools to effectively identify, assess and mitigate risks within digital landscapes.				
Assessment				
Internally assessed unit				
<b>Mandatory</b>	<b>Graded P/M/D</b>	<b>Level 4</b>	<b>15 credits</b>	<b>60 GLH</b>

Learning outcomes (LOs)	Mandatory teaching content
1. Examine operating system security features	<p><b>Knowledge:</b></p> <p>The features and functions of common OS:</p> <ul style="list-style-type: none"> <li>desktop – Windows, macOS, Linux, Kali Linux</li> <li>server – Windows server, Linux server</li> </ul> <p>The specific security features and their functionality within each OS</p>
2. Assess risk management in cyber security	<p><b>Knowledge:</b></p> <p>Scope of cyber security risk assessment</p> <p>Types of risk assessment methodologies (for example, fault tree analysis)</p> <p>Risk assessment process to support cyber security audits:</p> <ul style="list-style-type: none"> <li>define scope</li> <li>identification of threats and vulnerabilities</li> <li>likelihood of occurrence</li> <li>impact on architecture and services</li> <li>prioritisation based on analysis of likelihood and impact</li> <li>develop a risk treatment plan</li> <li>develop an assurance plan</li> <li>continuous improvement</li> </ul> <p>The role of risk owners/asset owners in risk response</p> <p>Documentation used to support the recording of risk treatment:</p> <ul style="list-style-type: none"> <li>risk assessment</li> <li>risk matrix</li> <li>risk register</li> </ul> <p>Impact on compliance with cyber security standards</p>

Learning outcomes (LOs)	Mandatory teaching content
	<p><b>Skills:</b></p> <p>Apply the risk assessment process to identify security risks and vulnerabilities to meet requirements</p> <p>Complete documentation as required</p> <p>Apply risk assessment methodology against a recognised security standard</p> <p>Suggest risk treatment solutions</p>

### Grading criteria

Learning outcomes (LOs)	Pass	Merit	Distinction
<b>LO1:</b> Examine operating system security features	<b>P1:</b> Describe fundamental security features offered by different operating systems	<b>M1:</b> Explain how the choice of operating system impacts an organisation's overall security posture	
<b>LO2:</b> Assess risk management in cyber security	<b>P2:</b> Define the scope of cyber security risk assessment and identifies common risk assessment methodologies	<b>M2:</b> Explain how risk assessment documentation supports risk treatment decisions and suggests appropriate risk treatment options	<b>D1:</b> Design a comprehensive risk assessment plan, tailoring it to meet the requirements of a recognised cyber security standard
	<b>P3:</b> Apply a basic risk assessment process to identify security risks and vulnerabilities in a given scenario	<b>M3:</b> Apply a risk assessment process, analysing results, and prioritising risks based on likelihood and impact	<b>D2:</b> Justify proactive risk treatment strategies, considering both technical and organisational countermeasures

## Unit 06 Cyber security management (K/651/0938)

Unit summary				
This unit immerses learners in the strategic realm of overseeing and organising cyber security operations within organisations. This unit empowers learners to bridge the gap between employer and end user requirements, whilst also mastering the principles of cyber security processes in incident investigation.				
Assessment				
Internally assessed unit				
<b>Mandatory</b>	<b>Graded P/M/D</b>	<b>Level 4</b>	<b>15 credits</b>	<b>60 GLH</b>

Learning outcomes (LOs)	Mandatory teaching content
1. Analyse employer and end user requirements	<p><b>Knowledge:</b></p> <p>Approaches used to analyse employer/end user requirements</p> <p>How employer/end user requirements inform security objectives:</p> <ul style="list-style-type: none"> <li>• stakeholder type</li> <li>• access levels</li> <li>• geographical location (UK or international)</li> <li>• potential vulnerabilities</li> <li>• potential threats</li> <li>• cost implications</li> </ul> <p>Development of a security case to meet employer/end user requirements:</p> <ul style="list-style-type: none"> <li>• functional security requirements:                             <ul style="list-style-type: none"> <li>○ authentication</li> <li>○ authorisation backup</li> <li>○ targets/achievements</li> <li>○ server clustering</li> <li>○ redundant backup servers</li> </ul> </li> <li>• non-functional security requirements:                             <ul style="list-style-type: none"> <li>○ robustness</li> <li>○ scalability</li> <li>○ performance</li> <li>○ architectural requirements</li> <li>○ reliability</li> <li>○ data integrity</li> </ul> </li> </ul> <p><b>Skills:</b></p> <p>Analyse employer/end user requirements to identify security objectives whilst taking into account threats and business context</p> <p>Develop a security case and propose justified security measures</p>

Learning outcomes (LOs)	Mandatory teaching content
	<p>Analyse functional and non-functional security requirements of a security case against relevant design requirements:</p> <ul style="list-style-type: none"> <li>• usability</li> <li>• cost</li> <li>• size</li> <li>• weight</li> <li>• power</li> <li>• heat</li> <li>• supportability</li> </ul> <p>Identify conflicting security requirements and propose justified resolution (for example, trade-off between cost and potential outcome)</p>
<p>2. Apply principles of incident investigation in cyber security management</p>	<p><b>Knowledge:</b></p> <p>Stages of the cyber incident response process:</p> <ul style="list-style-type: none"> <li>• triage</li> <li>• analyse</li> <li>• contain or mitigate</li> <li>• remediate or eradicate</li> <li>• recover</li> <li>• review</li> </ul> <p>Stages of the incident management process:</p> <ul style="list-style-type: none"> <li>• oversee</li> <li>• communicate</li> <li>• engage support</li> <li>• escalate</li> <li>• report</li> <li>• notify</li> <li>• lessons learned</li> </ul> <p>Digital forensics in incident investigations:</p> <ul style="list-style-type: none"> <li>• acquisition</li> <li>• preservation</li> <li>• examination</li> <li>• analysis and reporting</li> </ul> <p>The relationship between cyber incident response, incident management processes and digital forensics</p>

## Grading criteria

Learning outcomes (LOs)	Pass	Merit	Distinction
<b>LO1:</b> Analyse employer and end user requirements	<b>P1:</b> Describe stakeholder types, access levels, location, vulnerabilities, threats, and cost impact security objectives	<b>M1:</b> Explain how functional and non-functional requirements align with design constraints	<b>D1:</b> Critically evaluate different approaches for analysing requirements, selecting the most suitable for a given scenario
	<b>P2:</b> Identify employer/end user requirements to support specific security objectives, considering threats and business context	<b>M2:</b> Develop a security case, proposing appropriate security measures and providing basic justifications for their choices	<b>D2:</b> Develop a comprehensive security case with well-justified security measures, demonstrating a holistic understanding of security needs
	<b>P3:</b> Develop a security case including relevant security measures		
<b>LO2:</b> Apply principles of incident investigation in cyber security management	<b>P4:</b> Describe the stages of cyber incident response and incident management processes	<b>M3:</b> Analyse how incident response, management, and forensic processes work together to effectively handle cyber incidents	<b>D3:</b> Critically evaluate the effectiveness of different incident response and management strategies for various incident types, providing recommendations for the future



## 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 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

#### Competence/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

## Section 3: explanation of terms

This table explains how the terms used at level 4 in the content are applied to this qualification (not all verbs are used in this qualification).

<b>Analyse</b>	Break the subject or complex situations into separate parts and examine each part in detail. Identify the main issues and show how the main ideas are related to practice and why they are important. Reference to current research or theory may support the analysis.
<b>Critically analyse</b>	This is a development of 'analyse' which explores limitations as well as positive aspects of the main ideas in order to form a reasoned opinion.
<b>Clarify</b>	Explain the information in a clear, concise way showing depth of understanding.
<b>Classify</b>	Organise accurately according to specific criteria.
<b>Collate</b>	Collect and present information arranged in sequence or logical order that is suitable for purpose.
<b>Compare</b>	Examine the subjects in detail, consider and contrast similarities and differences.
<b>Critically compare</b>	This is a development of 'compare' where the learner considers and contrasts the positive aspects and limitations of the subject.
<b>Consider</b>	Think carefully and write about a problem, action or decision showing how views and opinions have been developed.
<b>Demonstrate</b>	Practical application of an element/content to show that you understand theories/concepts in a practical sense.
<b>Describe</b>	Provide a broad range of detailed information about the subject or item in a logical way.
<b>Discuss</b>	Write a detailed account that includes contrasting perspectives.
<b>Draw conclusions (which...)</b>	Make a final decision or judgement based on reasons.
<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. Apply current research or theories to support the evaluation.
<b>Critically evaluate</b>	This is a development of 'evaluate' where the learner debates the validity of claims from the opposing views and produces a convincing argument to support the conclusion or judgement.

<b>Examine</b>	Look closely at something. Think and write about the detail, and question it where appropriate.
<b>Explain</b>	Apply reasoning to account for how something is or to show understanding of underpinning concepts. Responses could include examples to support these reasons.
<b>Explore</b>	Consider an idea or topic broadly, searching out related and/or particularly relevant, interesting or debatable points.
<b>Identify</b>	Apply an in-depth knowledge to give the main points accurately (a description may also be necessary to gain higher marks when using compensatory marking).
<b>Investigate</b>	To inquire into (a situation or problem) to explore solutions.
<b>Justify</b>	Give a detailed explanation of the reasons for actions or decisions.
<b>Perform</b>	Present/enact/demonstrate practically.
<b>Reflect</b>	Learners should consider their actions, experiences or learning and the implications of these in order to suggest significant developments for practice and professional development.
<b>Review and revise</b>	Look back over the subject and make corrections or changes based on additional knowledge or experience.
<b>Summarise</b>	Give the main ideas or facts in a concise way to develop key issues.

## 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:

- Qualification Factsheet

### Useful websites

Centres may find the following websites helpful for information, materials and resources to assist with the delivery of this qualification:

- [www.instituteforapprenticeships.org](http://www.instituteforapprenticeships.org)
- [www.legislation.gov.uk](http://www.legislation.gov.uk)
- [www.ncsc.gov.uk](http://www.ncsc.gov.uk)
- [www.nist.gov](http://www.nist.gov)
- [www.owasp.org](http://www.owasp.org)
- [www.cisco.com](http://www.cisco.com)
- [www.wireshark.org](http://www.wireshark.org)

These links are provided as sources of potentially useful information for delivery/learning of this subject area. NCFE does not explicitly endorse these websites or any learning resources available on these websites. For official NCFE-endorsed learning resources, please see the additional and teaching materials sections on the qualification's page on the NCFE website.

### 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 2024 All rights reserved worldwide.**

DRAFT/Version 1.0 May 2024

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	Credit	GLH
Unit 01	Y/651/0932	Principles of cyber security	4	20	105
Unit 02	D/651/0934	Cyber security architecture	4	30	120
Unit 03	F/651/0935	Legislation, policies and procedures in cyber security	4	10	45
Unit 04	H/651/0936	Threat intelligence in cyber security	4	30	120
Unit 05	J/651/0937	Risk assessment in cyber security	4	15	60
Unit 06	K/651/0938	Cyber security management	4	15	60

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