Qualification specification

NCFE Level 3 Certificate in Cyber Security Practices
QN: 603/5762/9

Version 1.4 January 2024

Contents

Summary of changes

Version	Publication date	Summary of amendments
v1.0	July 2020	First publication
v1.1	March 2022	p.24, reference to Mitigations amended from assessment criteria 1.3 to 1.4.
v1.2	June 2022	Further information added to the how the qualification is assessed section to confirm that 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. Information added to the entry guidance section to advise that registration is at the discretion of the centre, in accordance with equality legislation and should be made on the Portal. Information added to the support handbook section about how to access support handbooks. GDPR legislation updated to UK General Data Protection Regulation (UK GDPR).
v1.3	July 2023	Information regarding UCAS added to About this qualification, Qualification Summary.
v1.4	January 2024	Wording amended in bullet point describing digital devices in the Resource requirements section.

Section 1

About this qualification

About this qualification

This Qualification Specification contains details of all the units and assessments required to complete this qualification.

To ensure that you are using the most up-to-date version of this Qualification Specification, please check the version number and date in the page footer against that of the Qualification Specification on the NCFE website.

If you advertise this qualification using a different or shortened name, you must ensure that learners are aware that their final certificate will state the full regulated qualification title.

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
- 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.

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.

Qualification summary	
Qualification title	NCFE Level 3 Certificate in Cyber Security Practices
Qualification number (QN)	603/5762/9
Aim reference	60357629
Total Qualification Time (TQT)	220
Guided Learning Hours (GLH)	150
Minimum age	16
UCAS	This qualification has been allocated UCAS points. Please refer to the UCAS website for further details of the points allocation and the most up-to-date information.
Qualification purpose	This qualification is designed to provide learners with knowledge and skills relating to cyber security practices. It will provide the learner with a chance to develop knowledge and learn practical skills which can be used to seek employment or proceed into study at a higher level.
Aims and objectives	This qualification aims to: • focus on the study of the practices within cyber security • offer breadth and depth of study, incorporating a key core of knowledge • provide opportunities to acquire a number of practical skills. The objective of this qualification is to: • provide the learner with an opportunity to develop knowledge and skills relating to cyber security practices.
Work/industry placement experience	Work/industry placement experience is not required.
Real work environment (RWE) requirement/ recommendation	Where the assessment requirements for a unit allow, it is essential that organisations wishing to operate a RWE do so in an environment which 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.
Assessment method	Internally assessed and externally quality assured portfolio of evidence.

Progression including job roles (where applicable)	Learners who achieve this qualification could progress to: • Level 4 Diploma in Cyber Security • Level 4 Certificate for IT Professionals • Level 4 Certificate in Information and Cyber Security Foundations • Level 4 Certificate in Cyber Security and Intrusion for Business.
Regulation information	This is a regulated qualification. The regulated number for this qualification is 603/5762/9.
Funding	This qualification may be eligible for funding. For further guidance on funding, please contact your local funding provider.

Entry guidance

This qualification will provide the learner with a chance to develop knowledge and skills relating to cyber security practices with the view to seeking employment or proceeding to further study in this area.

Registration is at the discretion of the centre, in accordance with equality legislation, and should be made on the Portal. This qualification is suitable for learners aged 16 and above.

There is no specific prior knowledge a learner must have for this qualification. However, learners may find it helpful if they’ve already achieved a Level 2 Digital Skills or Information Technology qualification.

Centres are responsible for ensuring that this qualification is appropriate for the age and ability of learners. They need to make sure that learners can fulfil the requirements of the learning outcomes and comply with the relevant literacy, numeracy and health and safety aspects of this qualification.

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

Achieving this qualification

To achieve this qualification, learners must successfully demonstrate their achievement of all learning outcomes of the units as detailed in this Qualification Specification. A partial certificate may be requested for learners who do not achieve their full qualification but have achieved at least one whole unit.

Units

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

The regulated unit number is indicated in brackets for each unit (eg M/100/7116) within Section 2.

☆ 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.

The units below may be available as stand-alone unit programmes. Please visit our website for further information.

Mandatory units

Unit number	Regulated unit number	Unit title	Level	GLH
☆ Unit 01	A/618/0866	Understand cyber security principles	3	30
Unit 02	F/618/0867	Threat intelligence in cyber security	3	30
Unit 03	J/618/0868	Cyber security testing, vulnerabilities and controls	3	30
Unit 04	L/618/0869	Cyber security incident response	3	30
☆ Unit 05	J/618/0871	Understand legislation and ethical conduct within cyber security	3	20
Unit 06	L/618/0872	Professional skills and behaviours for cyber security	3	10

Progression to higher level studies

This qualification aims to provide learners with a number of progression options, including higher level studies at university or FE colleges. The skills required to progress to higher academic studies are different from those required at Levels 1 and 2. Level 3 qualifications enable the development of these skills. Although there is no single definition of higher level learning skills, they include:

- checking and testing information
- supporting points with evidence
- self-directed study
- self-motivation
- thinking for yourself
- analysing and synthesising information/materials
- critical thinking and problem solving
- working collaboratively
- reflecting upon learning and identifying improvements.

Level 3 criteria can require learners to **analyse**, **draw conclusions**, **interpret** or **justify**, which are all examples of higher level skills. This means that evidence provided for the portfolio will also demonstrate the development and use of higher level learning skills.

If you need any further information, please refer to the NCFE website.

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:

- an internally assessed portfolio of evidence which is assessed by centre staff and externally quality assured by NCFE.

Unless stated otherwise in this qualification 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

Each learner must create a portfolio of evidence generated from appropriate assessment tasks, which demonstrates achievement of all the learning outcomes 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.

Internally assessed work should be completed by the learner in accordance with the Qualification Specification.

The Tutor must be satisfied that the work produced is the learner's own.

A centre may choose to create their own internal assessment tasks. The tasks should**:**

- be accessible and lead to objective assessment judgements
- permit and encourage authentic activities where the learner's own work can be clearly judged
- refer to Course File Documents on the NCFE website.

Supervision of learners and your role as an Assessor

Guidance on how to administer the internal assessment and the support you provide to learners can be found on the NCFE website.

Section 2

Unit content and assessment guidance

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 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 our Quality Assurance team.

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

For further information or guidance about this qualification, please contact our Customer Support team.

Unit 01 Understand cyber security principles (A/618/0866)

Unit summary	The learner will gain an understanding of cyber security and the consequences and implications of inadequate cyber security. They will understand key terminology and the motivations of good and bad actors. They will also investigate the advantages and disadvantages of security by design.
Guided learning hours	30
Level	3
Mandatory/optional	Mandatory

Learning outcome 1

The learner will:

1 Understand cyber security

The learner can:

1.1 Describe the **concepts of cyber security**
1.2 Explain the importance of cyber security
1.3 Describe the **consequences and implications** of inadequate cyber security

Learning outcome 2

The learner will:

2 Understand core terminology and key aspects of cyber security

The learner can:

2.1 Define **core terminology** used in cyber security
2.2 Explain the terms **good actors** and **bad actors**
2.3 Distinguish typical behaviours of good actors and bad actors
2.4 Explain the **motivations** of good actors and bad actors
2.5 Identify **key sectors** that are most vulnerable to a cyber-attack
2.6 Compare the motivations for a cyber-attack in key sectors
2.7 Consider how an actor may carry out a cyber-attack

Learning outcome 3

The learner will:

3 Understand security by design principles

The learner can:

3.1 Describe the term security by design
3.2 Explore the principles of security by design
3.3 State the consequences of not considering cyber security during the design phase
3.4 Evaluate the advantages and disadvantages of security by design

Assessment guidance

Delivery and assessment
1.1 **Concepts of cyber security** - the learner should cover as a minimum: • security • identity • confidentiality • integrity • availability • threat • vulnerability • risk • hazard. 1.3 **Consequences and implications** - must include, but are not limited to, unauthorised access to distribution of or loss of: • sensitive data • personally identifiable information (PII) • protected health information (PHI) • personal information • intellectual property • industry information systems. 2.1 **Core terminology –** as a minimum learners must define the following: • malicious software • distributed denial of service (DDoS) • cloud • software • domain • exploit • breach • firewall • encryption • Bring Your Own Device (BYOD) • penetration testing (pen testing). 2.2 **Good and bad actors** - must include, but is not limited to**:** • bad – ex employee, black hat, script kiddies, hacktivist • good – white hat, certified penetration tester. 2.4 **Motivations** - must include, but are not limited to: • bad actor – financial gain, terrorism, political motivation, reputation, disruption, respect, thrill seeking

- good actor – ethical, job role, improve things, innovation, challenge of being better than a black hat.

2.5 **Key sectors** must include, but are not limited to:

- health
- manufacturing
- finance
- government agencies and departments
- educational institutions.

2.7 Learners must state the type of attack and how it can be carried out by the actor.

3.2 Learners could explore the principles set out by organisations such as the National Cyber Security Centre (NCSC), for example.

3.3 Learners should use the NCSC guidelines to help them to state the consequences of not considering cyber security during the design phase.

3.4 Suggested evidence of assessment could be in report format and could provide a piece of evidence for a learner’s portfolio. Learners could consider an example based on their surroundings (eg swipe card to enter and exit the building).

The Explanation of terms (Section 3) explains how the terms used in the unit content are applied to this qualification.

Types of evidence

Evidence could include:

- research
- learner report
- written or oral question and answer
- discussion
- assignment
- presentation.

Unit 02 Threat intelligence in cyber security (F/618/0867)

Unit summary	The learner will gain an understanding of threat intelligence, Open Source Intelligence, and the importance of using reliable sources of information. They will understand threat models and the effects of malicious software.
Guided learning hours	30
Level	3
Mandatory/optional	Mandatory

Learning outcome 1

The learner will:

1 Understand cyber threat intelligence

The learner can:

1.1 Identify key concepts of cyber threat intelligence
1.2 Explain the following terms in relation to cyber security:
- **threats**
- exploits
- **vulnerabilities**
- risk

1.3 Describe the threat intelligence lifecycle
1.4 Describe how to find out about emerging attack techniques and how to recognise them
1.5 Consider what could be included in **Open Source Intelligence** data sets
1.6 Explain why it is important to only use reliable and valid sources of Open Source Intelligence information
1.7 Explain the importance of using reliable sources of information in relation to cyber security threats
1.8 Consider the current threat status and make possible recommendations based upon cyber threat intelligence information
1.9 Analyse relevant cyber threat intelligence information requirements for an organisation

Learning outcome 2

The learner will:

2 Understand threat models

The learner can:

2.1 Describe a range of **threat models**
2.2 Explain the steps within a threat model
2.3 Evaluate a threat model

Learning outcome 3

The learner will:

3 Understand malicious software

The learner can:

3.1 Identify types of **malicious software**
3.2 Describe the effects of different types of malicious software on an infected system
3.3 Describe the motives for using specific malicious software attacks
3.4 Identify how specific malicious software attacks are made more effective due to human factors

---

Learning outcome 4

The learner will:

4 Know about social engineering

The learner can:

4.1 Explain the term 'social engineering'
4.2 Give examples of how Open Source Intelligence can be used for social engineering
4.3 Describe ways a social engineering attack could take place

---

Assessment guidance

Delivery and assessment

1.1 Learners should be aware of the difference between the terms cyber threat and threat:

- cyber threat = phishing, etc
- threat = at risk.

1.2 **Threats** include, but are not limited to:

- malicious software
- data breaches
- Denial of Service (DoS) attacks.

Vulnerabilities must include, but are not limited to:

- flaws
- features
- user errors
- zero day.

1.5 **Open Source Intelligence** is also known as OSINT.

1.8 Learners could create a case study based on the information gathered, including recommended actions.

1.9 Learners must cover information on at least four different types of attack, a business to consumer (B2C) business is easier to focus on. Types of attack could include:

- phishing
- ransomware
- Denial of Service (DoS)/Distributed Denial of Service (DDoS)
- virus.

2.1 Learners must describe a minimum of three **threat models**. These could include, but are not limited to:

- STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege)
- PASTA (Process for Attack Simulation and Threat Analysis)
- LINDDUN (Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of information, Unawareness, Non-compliance)
- CVSS (Common Vulnerability Scoring System)
- Attack Trees.

3.1 **Malicious software** includes, but is not limited to:

- virus
- spyware
- trojan

• worms. 4.2, 4.3 Learners could undertake a case study to gather information using Open Source Intelligence and give examples of how the information could be used to carry out a social engineering attack. The Explanation of terms (Section 3) explains how the terms used in the unit content are applied to this qualification.

Types of evidence
Evidence could include: • research • learner report • written or oral question and answer • discussion • assignment • presentation

Unit 03 Cyber security testing, vulnerabilities and controls (J/618/0868)

Unit summary	The learner will gain an understanding of common types of testing in cyber security including mitigations following testing. They will understand vulnerabilities within cyber security and the steps to be taken when a vulnerability is identified. Learners will also gain knowledge of controls within cyber security and will be able to apply a basic control.
Guided learning hours	30
Level	3
Mandatory/optional	Mandatory

Learning outcome 1

The learner will:

1 Understand common types of testing in cyber security

The learner can:

1.1 Explain different types of **cyber security testing**
1.2 Identify why cyber security testing is important
1.3 Compare types of cyber security testing
1.4 Consider **mitigations** following cyber security testing
1.5 Explain why it is important to retest following any changes made
1.6 Explain how the outcomes of cyber security testing can be reported
1.7 Explain why the outcomes of cyber security testing must be reported

Learning outcome 2

The learner will:

2 Be able to reduce or remove potential cyber security vulnerabilities

The learner can:

2.1 Identify cyber security vulnerabilities
2.2 Demonstrate the steps to be taken when a vulnerability has been identified
2.3 Apply the correct response to the vulnerability
2.4 Develop an appropriate **communication** to mitigate future vulnerabilities

Learning outcome 3

The learner will:

3 Understand controls in cyber security

The learner can:

3.1 Identify cyber security controls
3.2 Explain a basic **cyber security framework**
3.3 Evaluate a cyber security framework

Learning outcome 4

The learner will:

4 Be able to apply a cyber security control

The learner can:

4.1 Explain how to apply controls
4.2 Implement a basic cyber security control
4.3 Justify the implementation of the chosen cyber security control
4.4 Explain why a control might not be applied

Assessment guidance

Delivery and assessment
1.1 **Cyber security testing** - must include, but is not limited to: • penetration • vulnerability • social engineering. 1.4 **Mitigations** must include, but are not limited to: • escalation • catching (including software updates, operating system updates, application updates) • user access control • high availability • staff training and awareness. 2.1 Learners should identify a range of cyber security vulnerabilities, taking into account cloud based and on-premises. The learner should also include common vulnerabilities in networks and systems. 2.2 Learners must demonstrate the steps to be taken when a vulnerability has been identified. Whilst the steps will vary, learners must include reference to organisational policies/procedures within the steps. 2.3 An example of a correct response could include patching or carrying out an update. 2.4 **Communication** documents could include an information leaflet or an email to management informing them of a vulnerability. 3.2 Learners must explain a basic **cyber security framework**. An example could be: • National Cyber Security Centre (NCSC), 10 Steps to Cyber Security • Centre for Internet Security (CIS) controls. 3.3 Example of an evaluation – an organisation may not encrypt the network traffic as if they encrypt it, they can’t read what is coming in via the network. What are the advantages and disadvantages of this? 4.1 Learners must explain how to apply a minimum of four cyber security controls, learners will have identified these in 3.1. 4.2 Learners must implement a basic cyber security control, an example of this could be demonstrating how to give access/deny access to a folder or drive. 4.4 Learners must explain reasons why a control might not be applied, for example, when is doing nothing a better option? The Explanation of terms (Section 3) explains how the terms used in the unit content are applied to this qualification.

Types of evidence
Evidence could include: • research • learner report • written or oral question and answer • discussion • assignment • presentation.

Unit 04 Cyber security incident response (L/618/0869)

Unit summary	The learner will gain an understanding of a cyber security incident response plan and checklist. They will also cover the knowledge required to be able to develop an incident post mortem report.
Guided learning hours	30
Level	3
Mandatory/optional	Mandatory

Learning outcome 1

The learner will:

1 Understand what is meant by a cyber security incident response plan

The learner can:

1.1 Describe what a cyber security incident response plan is used for
1.2 Explain when a cyber security incident response plan is used
1.3 Describe the stages of a cyber security **incident response lifecycle**

Learning outcome 2

The learner will:

2 Be able to develop a cyber security incident response plan

The learner can:

2.1 Explain why it is important to maintain an up to date cyber security incident log
2.2 Explain the steps to be included within a cyber security incident response plan
2.3 Explain why it is important to have a cyber security incident response plan
2.4 Develop a cyber security incident response plan for an organisation

Learning outcome 3

The learner will:

3 Be able to develop an incident post mortem report

The learner can:

3.1 Explain what is meant by incident post mortem
3.2 Explain the structure of an incident post mortem
3.3 Consider the importance of the following when carrying out an incident post mortem:

- integrity
- rigour
- discipline.

3.4 Create a post mortem report of an incident
3.5 Reflect upon the report and make recommendations based on the findings

Assessment guidance

Delivery and assessment
1.1, 1.2, 1.3 Learners should be aware that the cyber security incident response plan also contains a checklist which is a vital part of the plan. The description and explanation should include reference to the checklist as well as the overall plan. 1.3 **Incident response lifecycle** – there are a number of published incident response lifecycles available, learners must describe one of them. 3.4 The learner could be provided with a case study of a medium to large scale cyber incident for them to use to develop a post mortem report of the incident. The Explanation of terms (Section 3) explains how the terms used in the unit content are applied to this qualification.
Types of evidence
Evidence could include: • research • learner report • written or oral question and answer • discussion • assignment • presentation.

Unit 05 Understand legislation and ethical conduct within cyber security (J/618/0871)

Unit summary	The learner will gain an understanding of the legislation surrounding cyber security. They will understand international law relating to cyber security and the importance of information security standards, moving onto gaining an understanding of ethical conduct within cyber security.
Guided learning hours	20
Level	3
Mandatory/optional	Mandatory

Learning outcome 1

The learner will:

1 Understand legislation relating to cyber security

The learner can:

1.1 Describe how **legislation** impacts on cyber security
1.2 Explain trends in international law for cyberspace

Learning outcome 2

The learner will:

2 Understand information security standards

The learner can:

2.1 Identify **ISO standards** related to cyber security
2.2 Explain how ISO standards are used to support cyber security

Learning outcome 3

The learner will:

3 Understand ethical conduct within cyber security

The learner can:

3.1 Describe **ethical conduct** within cyber security
3.2 Identify **unethical conduct** within cyber security

Assessment guidance

Delivery and assessment
1.1 **Legislation**: The learner's description must cover a minimum of four pieces of legislation. Examples include, but are not limited to the following: • Computer Misuse Act 1990 • Official Secrets Act 1989 • Communications Act 2003 • Data Protection Act 2018/UK General Data Protection Regulation (UK GDPR) • Police and Criminal Evidence Act 1984 (PACE) • Directive on security of network and information systems (2016/1148) (known as the NIS Directive). Note that the above will change or be replaced over time and it is important that current and relevant legislation is covered. 1.2 Learners should give a basic explanation of the trends within international law for cyberspace. 2.1 **ISO standards**, for example: • ISO/IEC 27032:2012 • ISO/IEC 27000:2018 • ISO/IEC 27001:2013. Note that the above will change or be replaced over time and it is important that current and relevant standards are covered. 3.1 **Ethical conduct** must include, but is not limited to: • maintaining confidentiality • adherence to applicable laws • promoting information security • refraining from conflicts of interest. 3.2 **Unethical conduct** must include, but is not limited to: • sabotage • disclosing or misusing confidential information • maliciously injuring the reputation or prospects of an individual or business. The Explanation of terms (Section 3) explains how the terms used in the unit content are applied to this qualification.

Types of evidence
Evidence could include: • research • learner report • written or oral question and answer • discussion • assignment • presentation.

Unit 06 Professional skills and behaviours for cyber security (L/618/0872)

Unit summary	The learner will gain an understanding of the behaviours required for a career within cyber security, they will understand security clearance levels and possible employee screening checks that an employer might carry out. They will understand the skills required for a career within cyber security and will be able to assess their own skills. They will also understand the importance of continuous professional development.
Guided learning hours	10
Level	3
Mandatory/optional	Mandatory

Learning outcome 1

The learner will:

1 Understand behaviours required for a career in cyber security

The learner can:

1.1 Explain the importance of managing and promoting a positive digital identity
1.2 Describe possible **employee screening checks** that an employer might carry out
1.3 Consider **potential consequences** of unsatisfactory findings as a result of employer checks
1.4 Describe the following security clearance levels:

- BPSS (Baseline Personnel Security Standard)
- SC (Security Checked)
- DV (Developed Vetting)

1.5 Explain how bias can influence cyber security
1.6 Describe the benefits of a security by design mindset

Learning outcome 2

The learner will:

2 Be able to identify skills required for a career in cyber security

The learner can:

2.1 Identify skills required for a career in cyber security
2.2 Perform a personal skills analysis
2.3 Assess own skills against those required for a career in cyber security
2.4 Create a personal development plan

Learning outcome 3

The learner will:

3 Understand the importance of continuous professional development

The learner can:

3.1 Explain the term continuous professional development (CPD)
3.2 State methods of keeping up to date with industry knowledge
3.3 Explain why it is important to keep CPD up to date

Assessment guidance

Delivery and assessment

It is suggested that this unit is completed over time to allow the learner to develop skills and then reflect on progress made. The unit is 10 guided learning hours and it is estimated that non-guided learning hours will be around 20 hours.

1.1 Learners must include within their explanation that a digital image or footprint can be traced and used by third parties such as employers.

1.2 **Employee screening checks**, as a minimum learners must cover:

- a Disclosure and Barring Service (DBS) check (for criminal convictions, cautions etc)
- guilty by association check
- security checks such as terror lists, address checks, and employment verification checks
- credit checks.

1.3 **Potential consequences** can include, but are not limited to:

- unable to get security clearance (eg BPSS/SC/DV)
- unable to work in particular areas
- unable to work for high profile employers
- requirement to give an explanation of the results (eg non-payment of fine or association with an individual with a criminal record).

1.4 Learners must describe each of the security clearance levels including when they are used.

2.2 Learners must carry out an analysis of their skills. Learners could rate and rank their skills, utilise feedback from others, use an approach such as a SWOT (Strengths, Weaknesses, Opportunities and Threats) or SOAR (Strengths, Opportunities, Aspirations, Results) analysis.

2.4 Learners must create a personal development plan to address the areas for development identified within the personal skills analysis in 2.2 and assessment in 2.3, this must include SMART targets.

The Explanation of terms (Section 3) explains how the terms used in the unit content are applied to this qualification.

Types of evidence

Evidence could include:

- research
- learner report
- written or oral question and answer
- discussion
- assignment
- presentation.

Section 3

Explanation of terms

Explanation of terms

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

Apply	Explain how existing knowledge can be linked to new or different situations in practice.
Analyse	Break the subject down 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.
Clarify	Explain the information in a clear, concise way.
Classify	Organise according to specific criteria.
Collate	Collect and present information arranged in sequence or logical order.
Compare	Examine the subjects in detail and consider the similarities and differences.
Critically compare	This is a development of compare where the learner considers the positive aspects and limitations of the subject.
Consider	Think carefully and write about a problem, action or decision.
Demonstrate	Show an understanding by describing, explaining or illustrating using examples.
Describe	Write about the subject giving detailed information in a logical way.
Develop (a plan/idea which….)	Expand a plan or idea by adding more detail and/or depth of information.
Diagnose	Identify the cause based on valid evidence.
Differentiate	Identify the differences between two or more things.
Discuss	Write a detailed account giving a range of views or opinions.
Distinguish	Explain the difference between two or more items, resources, pieces of information.
Draw conclusions (which….)	Make a final decision or judgement based on reasons.
Estimate	Form an approximate opinion or judgement using previous knowledge or considering other information.
Evaluate	Examine strengths and weaknesses, arguments for and against, and/or similarities and differences. Judge the evidence from the different perspectives and make a valid conclusion or reasoned judgement. Reference to current research or theory may support the evaluation.
Explain	Provide detailed information about the subject with reasons showing how or why. Responses could include examples to support these reasons.

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

Section 4

Additional information

Additional information

Resource requirements

To assist in the delivery of this qualification, learners should have access to the following mandatory resources:

- a digital device for example, a desktop PC, laptop or tablet
- access to a storage medium prescribed by the organisation where the learner is in employment, or access to a storage medium where a simulated activity is undertaken
- web browser software/applications
- cyber security related software
- internet connectivity.

There is no requirement to use any specific software/applications. Centres are able to use any free or paid for software/applications as long as it allows learners to meet the assessment criteria.

Support for learners

Learner’s Evidence Tracking Log (LETL)

The LETL covers the mandatory units in this qualification and it can help learners keep track of their work. This document can be downloaded free of charge from the Qualifications page on the NCFE website. You do not have to use the LETL – you can devise your own evidence tracking document instead.

Useful websites

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

- National Cyber Security Centre https://ncsc.gov.uk
- International Organisation for Standardisation www.iso.org
- Centre for Internet Security https://www.cisecurity.org
- The NATO Cooperative Cyber Defence Centre of Excellence https://ccdcoe.org

Learning resources

We offer a wide range of learning resources and materials to support the delivery of our qualifications. Please check the Qualifications page on the NCFE website for more information and to see what is available for this qualification.

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
Websites: www.ncfe.org.uk

Version 1.4 January 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).

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