Qualification specification

NCFE Level 4 Diploma: Cyber Security Engineer

QN: 603/7748/3

Qualification summary

Qualification title	NCFE Level 4 Diploma: Cyber Security Engineer		
Ofqual qualification number (QN)	603/7748/3	**Aim reference**	60377483
Guided learning hours (GLH)	511	**Total qualification time (TQT)**	1200
Minimum age	18+		
Qualification purpose	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. 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 will give learners the skills, knowledge and behaviours to meet specific employer needs and industry requirements.		
Grading	Pass/merit/distinction		
Assessment method	Occupationally relevant simulated project assessments (ORSPA): Externally set, internally assessed and externally quality assured. Learners must complete 1 ORSPA as part of this qualification. Assignments: externally set, internally assessed and externally quality assured. Learners must complete 2 assignments as part of this qualification. Multiple choice question paper: externally set and marked. Learners must complete one multiple-choice question paper as part of this qualification.		
Apprenticeship standards	This HTQ content has been aligned with the Cyber Security Technologist Apprenticeship Standard. This HTQ is designed to be delivered as a standalone qualification which is an alternative to the apprenticeship. It does not form part of an apprenticeship.		

Contents

Section 1: introduction

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

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. For more information about HTQs, please visit www.instituteforapprenticeships.org/higher-technical-qualifications.

This HTQ content has been aligned with the Cyber Security Technologist 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 themes:

- cyber security architecture
- legislation
- threat intelligence
- security by design
- cyber security management
- systems and programming

Support handbook

This qualification specification must be used alongside the mandatory support handbook on the qualifications page on the NCFE website, which contains additional supporting information to help with the planning, delivery and assessment.

This qualification specification contains all of the qualification-specific information you will need that is not covered in the support handbook.

Entry guidance

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.

Entry is at the discretion of the centre.

There are no specific prior skills/knowledge a learner must have for this qualification. However, learners may find it helpful if they have already achieved a level 3 qualification.

Centres are responsible for ensuring that all learners are able to meet the requirements of the mandatory knowledge, skills and behaviours covered within this qualification.

Centres are responsible for ensuring that all learners are able to meet 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

Diploma

To be awarded this qualification, learners are required to successfully complete all mandatory themes.

To achieve this qualification, learners must successfully demonstrate their achievement of all content as detailed in this qualification specification.

Total qualification time (TQT) and independent learning hours for this qualification

The expectation for independent study (non-guided learning hours) is much greater at level 4 and 5 than for lower-level qualifications. This is reflected in the total qualification time (TQT) which has been set for this qualification. Independent study hours are essential for personal development and reflection, allowing learners to develop transferable skills such as time management, goal setting and self-motivation.

Some examples of activities which can be included in independent learning hours include:

- preparation for assessments
- practising skills
- reading articles/texts from a recommended reading list
- research and inquiry
- watching videos/listening to podcasts
- reviewing recordings/notes from study sessions
- peer activities, including peer feedback, meetings and discussions
- reflection

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

Staffing requirements

Centres delivering any of NCFE's qualifications must:

- have a sufficient number of appropriately qualified/experienced assessors to assess the volume of learners they intend to register
- have a sufficient number of appropriately qualified/experienced internal quality assurers to internally quality assure the anticipated number of assessors and learners
- ensure that all staff involved in assessment and internal quality assurance are provided with appropriate training and undertake meaningful and relevant continuing professional development
- implement effective internal quality assurance systems and processes to ensure all assessment decisions are reliable, valid, authentic, sufficient and current. This should include standardisation to ensure consistency of assessment
- provide all staff involved in the assessment process with sufficient time and resources to carry out their roles effectively

Resource requirements

Providers must ensure that the learner has access to the necessary materials, resources and workspaces for delivery and assessment.

- computer
- internet access
- audio/visual recording equipment
- software:
  - word processing (for example, MS Word, Google Docs)
  - presentation (for example, MS PowerPoint, Google Slides)
  - spreadsheet (for example, MS Excel, Google Sheets)
  - project management (for example, MS Excel, MS Project)
  - programming software (for example, TextEdit)
  - web browsers (for example, Chrome, Firefox, Edge)
  - web application development (for example, WAMP, MAMP)
  - simulated network software (for example, Packet Tracer)

Real work environment (RWE) recommendation

Where the assessment requirements for a qualification allow, it is essential that centres 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.

The assessment consists of 4 components:

- ORSPA:
  - cyber security report and recommendations
- controlled assessments:
  - on-programme assignments
  - practical scenarios
- multiple-choice question paper

Resubmission

For the ORSPA, one resubmission will be allowed for learners who fail a component at the first attempt. In these circumstances, learners can only achieve a pass grade for the relevant components.

Resit

Learners may resit a component that is graded as not yet achieved. There is no limit on the number of resit attempts, however the assessments are only offered once per year.

Learners must have completed all assessment components to gain the NCFE Level 4 Diploma: Cyber Security Engineer (603/7748/3).

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

For the delivery of assessments please refer to the centre guidance and sample assessment materials found on our website.

External assessment

Each learner is required to undertake 4 external assessments.

External assessments are set by NCFE and marked by the centre, except in the case of the multiple-choice question paper which is marked by NCFE. The assessment assesses learners' knowledge, skills and behaviours from across the qualification content.

Assessment	Themes	Knowledge and skills statements
Multiple-choice question paper	1, 2, 3, 4, 5 and 6	K1.1, K1.2, K1.3, K1.4, K1.5, K1.6, K1.7, K1.9, K1.12, K1.13, K1.15, K1.16, K2.1, K2.2, K2.3, K3.2, K3.4, K3.5, K5.1, K5.2, K6.1
Controlled assessment: on programme assignments	1, 2, 3 and 4	K1.2, K1.3, K1.4, K1.5, K1.6, K1.7, K2.1, K2.2, K3.1, K3.2, K3.3, K3.4, K3.5 S3.1, S3.2, S3.3, S3.4, S3.5, S4.1, S4.2, S4.3, S4.4
ORSPA: cyber security report and recommendations	1, 2, 3 and 5	K1.2, K1.8, K1.9, K1.11, K1,12, K1.13, K1.14, K1.15, K2.1, K2.2, K2.3, K3.2, K5.1, K5.2 S1.1, S1.2, S3.1, S3.4, S5.1, S5.2
Controlled assessment: practical scenarios	1, 3, 4, 5 and 6	K1.1, K1.2, K1.3, K1.4, K1.5, K1.6, K1.7, K1.8, K1.9, K1.10, K1.11, K1.12, K1.13, K1.14, K1.15, K3.1, K3.2, K3.3, K3.4, K3.5, K5.1, K5.2, K6.1 S1.1, S1.2, S3.1, S3.2, S3.3, S3.4, S3.5, S4.1, S4.2, S4.3, S4.4, S5.1, S5.2, S6.1

The external assessment consists solely of or of a combination of:

- set date and time (invigilated) – NCFE specifies the exact date and time that the external assessment must be administered in the centre
- assessment window (supervised) – the centre arranges supervised periods of external assessment within a set window
- independent self-study (ORSPAs) – these are completed independently by learners

The assessment is administered under specified assessment conditions.

Assessment	Hours/Timings
1. Multiple-choice question paper	1 hour
2. On programme assignments	8 hours
3. ORSPA: cyber security report and recommendations	16 hours (delivered in a 4 week window)

4. Practical scenarios	14 hours

For further information, centres should refer to the regulations for the conduct of external assessments and qualification specific instructions for delivery documents, available on the policies & documents page on the NCFE website.

Where qualifications have external assessment, centres must have entered learners using the Portal to access the assessment.

Centres must enter learners at least 10 working days in advance of the assessment window to avoid late entry fees.

If applicable, pre-release material will be made available by NCFE in advance of the assessment. All centres with entries will be notified.

The external assessment material will be sent out in time for the start of the assessment. Assessment materials must be kept secure at all times.

Enquiries about results

All enquiries relating to learners' results must be submitted in line with our enquiries and appeals about results and assessment decisions policy, which is available on the policies & documents page on the NCFE website.

Assessment windows

For assessments sat in windows, the centre must enter learners to the specified window. This will be either a set date and time assessment or a window in which the assessment will be completed.

For qualifications with 'entry on registration', the centre will choose the assessment window at the point of registering the learner.

The NCFE Level 4 Diploma: Cyber Security Engineer consists of four assessments with the following windows:

Assessment	Window	Themes covered
1. Multiple-choice question paper	Fixed date and time examination in December	Themes 1, 2, 3, 4, 5 and 6
2. On programme assignments	2 week window, starting 1 February	Themes 1, 2, 3 and 4
3. ORSPA: cyber security report and recommendations	4 week window, starting 1 April	Themes 1, 2, 3 and 5
4. Practical scenarios	2 week window, starting 1 June	Themes 1, 3, 4, 5 and 6

Assessment windows have been set to ensure centres have time to deliver relevant content before the assessment is sat. In each case, centres should review the coverage, including detailed coverage listed in the external assessment table above, to plan their delivery.

Types of external assessment

Each learner is required to undertake an externally set multiple-choice question paper/short-answer question paper/assignment/project.

Multiple-choice question (MCQ) paper

The multiple-choice question paper will be assessed on a set date and time specified by NCFE. The MCQ assessment for the qualification is available through our online assessment service.

Online assessment

For more information about how to get started with online assessment, please go to the delivery and learner support page on the NCFE website.

For instructions on conducting online external assessments, please refer to our regulations for the conduct of external assessments and qualification specific instructions for delivery documents, available on the policies & documents page on the NCFE website.

External assessment conditions

For more information on external assessment conditions, please see the regulations for the conduct of external assessments and qualification specific instructions for delivery on the policies & documents page on the NCFE website.

To access the external assessment, centres need to ensure that learners are entered for the external assessment through the online assessment platform as appropriate.

Please refer to the external assessment timetable on the NCFE website for specific dates for assessment windows.

There is no limit to the number of attempts a learner can have on the multiple-choice question paper.

For instructions on conducting external assessments, please refer to our regulations for the conduct of external assessments and qualification specific instructions for delivery documents, available on the policies & documents page on the NCFE website.

Grading information

To achieve the qualification, learners must achieve at least a pass in all of the assessments (or a near pass in the multiple-choice question paper).

The learner's final qualification grade is made up of an aggregation of their achievement in each of the assessments, based on the assessments' proportional importance to the final grade – this is represented as a percentage weighting.

Assessments are assigned an incremental weighting based on their percentage weighting. Each grade is assigned a points value: pass = 1, merit = 3 and distinction = 5. The value of each grade in each assessment is determined by multiplying the incremental value by the grade value.

Assessment	% weighting	Incremental weighting	Distinction		Merit		Pass	
			Grade value	Points	Grade value	Points	Grade value	Points
1. Multiple-choice question paper	15%	3	5	15	3	9	1	3
2. On programme assignments	25%	5	5	25	3	15	1	5
3. ORSPA: cyber security report and recommendations	25%	5	5	25	3	15	1	5
4. Practical scenarios	35%	7	5	35	3	21	1	7

The points achieved in each assessment are summed and the total is used to determine the overall qualification grade based on the following values:

Points score	Grade
80–100	Distinction
40–79	Merit
20–39	Pass
0–19	NYA

Assessment grading

Assessment tasks for the controlled assessments and ORSPAs are set by NCFE and assessed by the centre. Multiple-choice question papers are externally marked by NCFE.

With the exception of some practical tasks, where a mark-based approach is taken, NCFE's controlled assessments and ORSPAs are judged by the centre using level of response grade descriptors, ranging from zero evidence (and therefore no achievement) through near pass, pass, merit and distinction standards. In each case, these descriptors are written to reflect the mid-point, rather than the borderline, of that standard.

This approach, including the use of a near pass grade, allows for a degree of compensation across the tasks and assessments, to ensure that the final grade fairly reflects the learner's achievement against the standard.

Overall grade boundaries are set at a mid-point between bands. For example, the overall pass boundary lies at the mid-point between bands 1 and 2, which are aligned to the grading standard associated with the near pass and pass grades respectively. The near pass grade allows learner evidence that may be below the pass standard, but still represents some achievement, to be recognised in the final assessment grade.

The grade boundaries are aligned to the qualification level grade descriptors at pass and distinction. These descriptors have been written as a description of the typical or mid-point pass and distinction standard required in the context of the purpose of the qualification.

This means that a learner will have to demonstrate the grade standard in at least half of the tasks, with the remaining half being demonstrated at the band below, in order to achieve the minimum requirement for the grade. The grading model also allows a compensatory approach to be taken for all possible combinations of assessment decisions. For example, while a learner will achieve an overall distinction if they achieve 50% of tasks at distinction standard and 50% at merit, they can also achieve an overall distinction if they achieve a pass standard in some tasks but compensate for this by achieving more than 50% of tasks at distinction.

A grading calculator has been provided to produce assessment grades based on task-based assessment decisions. Centres should use this calculator to calculate their overall assessment grades before submission of grades to NCFE (other than for the multiple-choice question paper, where relevant). Values have been provided in the tables below for information.

Assessment 1: multiple-choice question paper

The multiple-choice question paper consists of 40 marks, with the following default grade boundaries:

Grade	Boundary
NYA	0
N	20
P	25
M	30
D	35

Assessment 2: on programme assignments

Task	Weighting	Band			
		N	**P**	**M**	**D**
1	30%	6	12	18	24
2	30%	6	12	18	24
3	40%	8	16	24	32
Total	100%	20	40	60	80

Assessment 3: ORSPA: cyber security report and recommendations

Task	Weighting	Band			
		N	**P**	**M**	**D**
1	100%	20	40	60	80
Total	100%	20	40	60	80

Assessment 4: practical scenarios

Task	Weighting	Band			
		N	**P**	**M**	**D**
1	20%	4	8	12	16
2	20%	4	8	12	16
3	15%	3	6	9	12
4	20%	4	8	12	16
5A	15%	3	6	9	12
5B	10%	2	4	6	8
Total	100%	20	40	60	80

Qualification grade descriptors

The following descriptors represent the standard expected of a learner at the relevant grade. They describe the mid-point or typical standard for that grade (they do not attempt to describe the borderline pass or borderline distinction standard – rather the mid-point or typical standard for that grade):

Grade	Demonstration of attainment
Pass	The learner can apply the basic principles of cyber security to assess solutions that are appropriate and proportionate to identified risk scenarios.
	The learner can reference the main areas of the legislation and regulation environment in the UK that may influence cyber security within businesses.
	The learner can suggest technical cyber security mitigations with reference to the 7-layer OSI Model (for example, referencing that implementing Secure Socket Layer (SSL) security is applied at layer 6, the presentation layer).
	The learner should understand and be able to list the main ports and sockets associated with cyber security, and why certain ports and sockets are high risk and why their use should be avoided.
	The learner should be able to describe a basic network configuration, and the common routing protocols and factors which may affect the performance and security of that network.
	The learner must be able to explain the differences and advantages/disadvantages between physical and virtual networking.
	The learner should be able to discuss at least 2 reliable sources of cyber security architectures, standards and advice.
	The learner should be able to design a network for a business which implements basic security components in line with industry good practice guidance.
	The learner should be able to list the types of security controls that can be implemented (physical, technical, administrative) and be able identify at least one from each category in a business scenario.
	The learner should understand and be able to articulate how risk assessment and risk management may affect the technical controls implemented by a business.
	The learner should understand and be able to articulate why it is important to attain a balance between the people, process and technology elements of security controls.

	Using commercially available tools, the learner should be able to identify common vulnerabilities within a standard network configuration.
	The learner should be able to describe common forms of cyber-attack and the types of threat actors who may use these techniques. They should demonstrate the use of threat analysis processes or sources in identifying these potential threats.
	The learner should be able to identify the responsibilities of a cyber security engineer in the service management lifecycle.
	The learner should be able to identify the key security controls within one of the commonly used operating systems (Windows (PC and Server), macOS, Linux).
	The learner should be able to describe 2 practical applications of encryption within a business, and the importance of key management and recognised industry good practice approaches to key management.
	The learner should be able to describe common approaches to system monitoring and be able to explain the aims and objectives of system monitoring.
	The learner should be able to describe the common pitfalls experienced with system monitoring.
	The learner should be able to identify cross-site scripting (XSS), SQL injection and broken authentication vulnerabilities within a selection of code snippets.
Merit	The learner can apply complex principles of cyber security to assess solutions. They demonstrate an understanding of the link between risk management and the appropriateness and proportionality of solutions and how people, process and technology elements need to be balanced to ensure controls work effectively.
	The learner can reference some main areas of the legislation and regulation environment in the UK that may influence cyber security within businesses. They will also be able to reference areas of international law that businesses may need to consider, such as rules around encryption and data storage.
	The learner can suggest technical cyber security mitigations with reference to the 7-layer OSI Model (for example, referencing that implementing Secure Socket Layer (SSL) security is applied at layer 6, the presentation layer). They can also relate this to the TCP/IP Stack.
	The learner should understand and be able to list the majority of the ports and sockets associated with cyber security, and effectively cover why certain ports and sockets are high risk and why their use should be avoided.
	The learner should be able to describe a complex network configuration, and the necessary routing protocols and factors which may affect the performance and security of that network.

	The learner must be able to explain the differences and advantages/disadvantages between physical and virtual networking. They will also be able to describe the key security considerations for each option.

	The learner should understand and be able to discuss reliable sources of cyber security architectures, standards and advice.
	The learner should be able to design a network for a business which implements security components that are based on risk analysis, and provide solutions which are appropriate and proportionate and remain in line with industry good practice guidance.
	The learner should be able to list the types of security controls that can be implemented (physical, technical, administrative) and be able to identify at least 3 from each category in a business scenario.
	The learner should understand and be able to articulate how risk assessment and risk management may affect the technical controls implemented by a business.
	The learner should understand and be able to articulate why it is important to attain a balance between the people, process and technology elements of security controls.
	Using commercially available tools, the learner should be able to identify most of the common vulnerabilities within a standard network configuration. They should also be able to identify false positives in a network scan and explain how these may have manifested.
	The learner should be able to describe common forms of cyber-attack and the types of threat actors who may use these techniques. They should demonstrate the use of threat analysis processes and multiple information sources in identifying these potential threats.
	The learner should be able to explain the standard information technology infrastructure library (ITIL) service management framework, and identify the points at which the cyber security engineer should be involved and what their involvement should be.
	The learner should be able to identify the key security controls within at least 2 of the commonly used operating systems (Windows (PC and Server), macOS, Linux).
	The learner should be able to describe practical applications of encryption within a business, and the importance of key management and recognised industry good practice approaches to key management.
	The learner should be able to describe common approaches to system monitoring and be able to explain the aims and objectives of system monitoring.
	The learner should be able to describe the common pitfalls experienced with system monitoring. They will also be able to identify commonly acceptable solutions to these pitfalls.

	The learner should be able to identify at least 5 of the Open Web Application Security Project (OWASP) top 10 vulnerabilities within a selection of code snippets.

Distinction	The learner can apply advance principles of cyber security to assess solutions. They demonstrate an understanding of the link between risk management and the appropriateness and proportionality of solutions and how people, process and technology elements need to be balanced to ensure controls work effectively.
	The learner can reference the main areas of the legislation and regulation environment in the UK that may influence cyber security within businesses. They will also be able to reference areas of international law that businesses may need to consider, such as rules around encryption and data storage.
	The learner can suggest technical cyber security mitigations with reference to the 7-layer OSI Model (for example, referencing that implementing Secure Socket Layer (SSL) security is applied at layer 6, the presentation layer). They can also relate this to the TCP/IP Stack.
	The learner should understand and be able to list the main ports and sockets associated with cyber security, and why certain ports and sockets are high risk and why their use should be avoided.
	The learner should be able to describe a complex network configuration, and the necessary routing protocols and factors which may affect the performance and security of that network.
	The learner must be able to explain the differences and advantages/disadvantages between physical and virtual networking. They will also be able to describe the key security considerations for each option.
	The learner should understand and be able to discuss reliable sources of cyber security architectures, standards and advice.
	The learner should be able to design a network for a business which implements security components that are based on risk analysis and provide solutions which are appropriate and proportionate and remain in line with industry good practice guidance.
	The learners should be able to list the types of security controls that can be implemented (physical, technical, administrative) and be able identify at least 3 from each category in a business scenario.
	The learners should understand and be able to articulate how risk assessment and risk management may affect the technical controls implemented by a business.
	The learner should understand and be able to articulate why it is important to attain a balance between the people, process and technology elements of security controls.
	Using commercially available tools, the learner should be able to identify common vulnerabilities within a standard network configuration. They should also be able to identify false positives in a network scan and explain how these may have manifested.

	The learner should be able to describe common forms of cyber-attack and the types of threat actors who may use these techniques. They should demonstrate the use of threat analysis processes and multiple information sources in identifying these potential threats.

	The learner should be able to explain the standard information technology infrastructure library (ITIL) service management framework, and identify the points at which the cyber security engineer should be involved and what their involvement should be.
	The learner should be able to identify the key security controls within at least 2 of the commonly used operating systems (Windows (PC and Server), macOS, Linux).
	The learner should be able to describe practical applications of encryption within a business, and the importance of key management and recognised industry good practice approaches to key management.
	The learner should be able to describe common approaches to system monitoring and be able to explain the aims and objectives of system monitoring.
	The learner should be able to describe the common pitfalls experienced with system monitoring. They will also be able to identify commonly acceptable solutions to these pitfalls.
	The learner should be able to identify a range of the Open Web Application Security Project (OWASP) top 10 vulnerabilities within a selection of code snippets.

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

Section 2: qualification content

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

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

Behavioural framework

Embedded within higher technical qualifications 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 skills – that will be assessed as part of this higher technical qualification. Learners may also naturally demonstrate these behaviours elsewhere, beyond the listing below. All listed behaviours are subject to assessment.

B1: Logical – applies logical thinking
B2: Analytical – working with data effectively to see trends and patterns and draw meaningful conclusions
B3: Works independently and takes responsibility
B4: Shows initiative, being resourceful when faced with a problem and taking responsibility for solving problems within their own remit
B5: Thorough and organised
B6: Works effectively with a wide range of people in different roles, with a regard to inclusion and diversity policy
B7: Communicates effectively in a wide variety of situations
B8: Maintains a productive, professional and secure working environment
B9: Creative – taking a variety of perspectives, and 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									
Themes	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10
1: Cyber security architecture	K1.14 S1.1	S1.1	S1.1	K1.11 K1.13 S1.1	S1.1		S1.1	S1.1	S1.1 S1.2	K1.11 K1.12 K1.13 S1.1
2: Legislation										
3: Threat intelligence	K3.2 S3.1 S3.2 S3.4	S3.2 S3.4 S3.5	S3.1	K3.5	S3.2 S3.3 S3.4 S3.5	S3.2	S3.1 S3.2 S3.4	S3.2 S3.4	K3.1 S3.1	S3.1
4: Security by design	S4.1 S4.2 S4.3 S4.4		S4.1 S4.2 S4.4	S4.1 S4.2 S4.4	S4.1 S4.2 S4.4			S4.1 S4.2	S4.1 S4.2 S4.3 S4.4	S4.2 S4.3 S4.4
5: Cyber security management	S.5.1	S5.1 S5.2		S5.1		K5.1 S5.1	S5.1		S5.1	
6: Systems and programming	S6.1		S6.1							

Theme 1: Cyber security architecture

Knowledge – What you need to teach	

K1.1	**The learner must understand the principles of cyber security and their role within organisations and society**
	
	• principles of cyber security:
	  o CIA Triad:
	  ▪ confidentiality
	  ▪ integrity
	  ▪ availability
	  o IAAA:
	  ▪ identity
	  ▪ authentication
	  ▪ authorisation
	  ▪ audit
	  o non-repudiation:
	  ▪ accountability
	  ▪ applicable uses
	• role of cyber security principles:
	  o organisation:
	  ▪ aligns business objectives and security objectives
	  ▪ protects organisational reputation
	  ▪ supports compliance with legislation
	  ▪ protects organisational data
	  ▪ protects organisational assets:
	  • people
	  • hardware
	  • software
	  o society:
	  ▪ allows citizens to interact with digital services in a safe environment
	  ▪ protects personal data

K1.2	**The learner must understand the fundamentals of TCP/IP networking and the transmission of data between networked devices**
	
	• fundamentals of TCP/IP:
	  o Transmission Control Protocol (TCP):
	  ▪ connection oriented transmission
	  ▪ endpoints establish a synchronised connection prior to data transmission
	  ▪ receipt of data packet acknowledged by the receiving device
	  o User Datagram Protocol (UDP):
	  ▪ connectionless transmission between hosts
	  ▪ arrival and validation of segments at destination not verified
	  ▪ reliant on application validation
	  ▪ smaller overheads as header information is much smaller
	• transmission of data:
	  o TCP operation (three-way handshake):
	  ▪ synchronisation
	  ▪ segment structure
	  ▪ session structure
	  ▪ sequence (SYN) and acknowledgement (ACK) bits
	  o addressing and naming

- media access control (MAC) addresses
- IPv4
- IPv6
- Windows Internet Name Service (WINS)
- subnets and subnet masks
- network address translation (NAT)
- Dynamic Host Configuration Protocol (DHCP)
- Domain Naming System (DNS)
- Dynamic DNS (DDNS)

K1.3 **The learner must understand the utilisation of applications, protocols, services and devices within the layers of the TCP/IP/OSI models**

TCP/IP	**OSI**	**Layer**	**Applications, protocols and services**	**Devices**
Application layer	Application layer	7	Telnet, FTP, SMTP, DNS, DHCP, HTTP, POP3, NTP, IMAP, SNMP, HTTPS	
	Presentation layer	6	TLS, SSL, SSH	
	Session layer	5	NFS, SMB, SIP, NetBios	
Transport layer	Transport layer	4	TCP, UDP	Firewall
Network layer	Network layer	3	IPv4, IPv6, NAT, ICMP, RIP	Router
Network access layer	Data link layer	2	VLAN, VRF, MAC, LLC	Switch, bridge, wireless access point
	Physical layer	1	Physical connectivity	Cable, hub

K1.4 **The learner must understand the ports and protocols applied within the application layer of networking models**

TCP/UDP port	Protocol	Use
TCP:20/21	File Transfer Protocol (FTP)	Transmission of files between IP systems
TCP:23	Telnet	Remote access to communication systems
TCP:25	Simple Mail Transfer Protocol (SMTP)	Communication between mail servers
TCP/UDP:53	Domain Naming System (DNS)	Translation of device names to IP addressing
UDP:67/68	Dynamic Host Configuration Protocol (DHCP)	Dynamically assigning IP addresses and network configuration
TCP:80	Hypertext Transfer Protocol (HTTP)	Sending and receiving web client information
TCP:110	Post Office Protocol (POP3)	Retrieval and download of email messages to a client device from an email server
UDP:123	Network Time Protocol (NTP)	Clock synchronisation between computer systems
TCP:143	Internet Message Access Protocol (IMAP)	Management of email storage and access on a mail server
TCP/UDP:161/162	Simple Network Management Protocol (SNMP)	Collecting and organising information about managed devices on IP networks

TCP/UDP Port	Protocol	Use
TCP:3389	Remote Desktop Protocol (RDP)	Remote connection to a computer
TCP:22	Secure Shell Protocol (SSH)	Remote command line connection
UDP:69	Trivial File Transfer Protocol (TFTP)	Exchanges files between 2 TCP/IP machines
TCP/UDP:137/138/139	NetBIOS	Communication protocol within Local Area Network (LAN)
TCP/UDP:389	Lightweight Directory Access Protocol (LDAP)	Authentication of users
TCP:989/990	File Transfer Protocol (FTP) over Secure Sockets Layer (SSL)	Secure FTP server with SSL certificate
TCP:433	Hypertext Transfer Protocol Secure (HTTPS)	HTTP traffic encrypted with SSL/transport layer security (TLS)
UDP:520	Routing Information Protocol (RIP)	Calculates shortest route based on number of hops
TCP:179	Border Gateway Protocol (BGP)	Routes based on paths or manual configuration

K1.5 **The learner must understand routing protocols and the application within a TCP/IP network**

- dynamic routing protocols:
  - Routing Information Protocol (RIP):
    - RIPv1
    - RIPv2
  - Open Shortest Path First (OSPF) – calculates fastest route based on metric/cost
  - Border Gateway Protocol (BGP)
  - Intermediate System to Intermediate System (ISIS)
  - Enhanced Interior Gateway Routing Protocol (EIGRP)
- static routing:
  - static routes
  - default routes

	○ policy-based routing (PBR)
K1.6	**The learner must understand the factors which can affect network performance and the failure modes and error checking controls within TCP/IP** • network performance factors: ○ network latency – duration of sending packet from source to destination: ▪ impacts TCP traffic ▪ causes of latency: • distance between network devices • number of devices/hops between source and destination • performance and transfer rate of each device ○ network congestion – saturation of available bandwidth of a device or connection: ▪ packet transfer failure due to congestion ▪ causes of network congestion: • outdated hardware • bad configuration management • low bandwidth • border gateway protocols ○ network misconfiguration – misconfiguration of optimal configuration: ▪ causes of misconfiguration: • hardware failure • power failure • security breaches • failure modes and error checking: ○ TCP: ▪ delivery acknowledged by ACK segment ▪ corruption verified by checksum ▪ out-of-order segments identified until complete ▪ problem segments retransmitted following error detection ○ UDP: ▪ 16-byte checksum for error detection ▪ no error recovery ▪ optional in IPv4 ▪ mandatory in IPv6
K1.7	**The learner must understand TCP/IP techniques applied in virtualised networking** • techniques used in virtual networking: ○ virtual network interface cards (VNIC) ○ virtual IP addressing ○ virtual IP address takeover ○ internal virtual network ○ virtual local area network (VLAN) ○ virtual switching ○ virtual private network (VPN) ○ software-defined networking (SDN) ○ Multiprotocol Label Switching (MPLS) ○ virtual private LAN service (VPLS) • techniques for connecting virtual networks to physical networks: ○ Proxy Address Resolution Protocol (ARP) ○ network address translation (NAT) ○ TCP/IP routing

K1.8	**The learner must understand the types of security architecture and reputable sources of architecture patterns**
	
	• security architecture:
	  ○ The Open Group Architecture Framework (TOGAF)
	  ○ Sherwood Applied Business Security Architecture (SABSA)
	  ○ Open Security Architecture (OSA)
	  ○ National Institute of Standards and Technology (NIST)
	  ○ Ministry of Defence Architecture Framework (MODAF)
	  ○ Control Objectives for Information and Related Technology (COBIT)
	• sources of architecture patterns and guidance:
	  ○ National Cyber Security Centre (NCSC)
	  ○ National Institute of Standards and Technology (NIST
	  ○ vendor-specific

K1.9	**The learner must understand the types of cyber technology components which can be deployed using industry recognised good practice**
	
	• types of cyber security technology components:
	  ○ unified threat management (UTM)
	  ○ firewalls:
	  ▪ software
	  ▪ hardware
	  ○ intrusion prevention system (IPS)
	  ○ intrusion detection system (IDS)
	  ○ privacy access management
	  ○ identity access management
	  ○ secure communication – encryption
	  ○ proxies
	  ○ reverse proxies
	  ○ email filtering
	• implementation of hardware and software components in compliance with industry good practice:
	  ○ 18 CIS Controls
	  ○ Open Web Application Security Project (OWASP)
	  ○ NCSC
	  ○ SANS
	  ○ European Union Agency for Cyber Security (ENISA)
	• methods of documenting architecture:
	  ○ block definition diagram (BDD)
	  ○ data flow diagram (DFD)
	  ○ automated documentation

K1.10	**The learner must understand the function and features of network components and their role within a digital system**
	
	• network components:
	  ○ switch
	  ▪ switches data packets between devices on the same network
	  ▪ operates at OSI layer 2 – datalink layer
	  ▪ uses MAC address of the destination network adapter to determine where to send traffic

	▪ uses a MAC address table to record physical switch port and network adapter connections o router: ▪ routes data packets between devices on different networks, VLANs or sites ▪ operates at OSI layer 3 – network layer ▪ uses IP address of the destination device to determine where to send traffic ▪ uses a routing table to determine the route to the destination network o firewall: ▪ network perimeter security device ▪ monitors and controls all incoming and outgoing traffic o next-generation firewall (NGFW): ▪ functionality of a traditional firewall ▪ additional advance functionality (for example application firewalls, deep packet inspection, identity management, intrusion prevention) o wireless access: ▪ WPA2 ▪ WPA3 ▪ WEP
K1.11	**The learner must understand common vulnerabilities in digital systems** • physical network vulnerabilities: o insufficient physical security o insufficient access controls • network vulnerabilities: o misconfiguration o weak credentials o insufficient segregation • cloud vulnerabilities: o misconfiguration o weak credentials o insufficient access permissions o insecure application programming interface (APIs) o insufficient web application firewall (WAF) • operating system (OS)/software vulnerabilities: o operating software can be exploited to run malicious software o operating systems can be exploited to give elevated permissions • process vulnerabilities: o insufficient controls and documented procedures. o poor processes which allow for malicious or accidental loss of data
K1.12	**The learner must understand the concepts and types of cyber security attacks** • threat actors: o hackers/hacktivists: ▪ script kiddies o insiders o nation state o cyber criminals o terrorist organisations • motivations for cyber attacks: o political o social o environmental

- boredom
- challenge
- financial gain
- personal:
  - aggrieved employee
  - targeting a customer

- opportunity:
  - financial fluctuations
  - organisational changes:
    - staff
    - technology
  - political changes
  - mismanaged third-party services
  - company takeover or merge
- types of system-focused attacks:
  - denial of service (DoS)
  - distributed denial of service (DDoS)
  - SQL injection
  - zero-day exploit
  - DNS tunnelling
  - formjacking
  - cross-site scripting (XSS)
  - man in the middle (MITM) attacks
  - ransomware
  - remote access trojan (RAT)
  - malware
  - botnets
  - cryptojacking
  - DNS poisoning
  - spyware
  - VLAN hopping
  - backdoors
  - escalating privileges
  - port scanning
  - drive-by downloads
  - rootkits and bootkits
- types of human focused attacks:
  - social engineering:
  - phishing:
    - SMShing
    - vishing
    - angler phishing
    - spearphishing
    - whaling
  - footprinting
  - waterholing
  - doxing
  - intimidation techniques
  - impersonation of colleagues or officials
  - invoice payment fraud
  - malicious insider attack
    - aggrieved employee
    - negligent employee
    - recent leaver
    - incorrectly configured access controls

	▪ bribery ○ non-malicious insider attack: ▪ untrained staff (for example lack of awareness) ▪ poor systems design ▪ poor process design ▪ staff under pressure
K1.13	**The learner must understand the types and applications of defence controls to mitigate vulnerabilities and risks** • physical security controls: ○ perimeter fencing ○ security guards ○ security badges ○ alarms ○ CCTV • technical controls: ○ firewalls: ▪ pre-installed ▪ third-party ○ issue prevention ○ message parsing and validation ○ secure configuration ○ encryption ○ patch management ○ anti-virus software ○ back-ups ○ traffic filtering ○ least permissions and access • administrative controls: ○ policies ○ Privileged Access Management (PAM) ○ Intrusion Prevention System (IPS) ○ Intrusion Detection System (IDS) ○ Multiprotocol Label Switching (MPLS) ○ standard operating procedures ○ staff training ○ visitor access ○ multi-factor authentication (MFA)
K1.14	**The learner must understand the stages of the service lifecycle and its application within service management practices** • service lifecycle stages: ○ service strategy: ▪ strategy management ▪ financial management for IT services ▪ demand management ▪ business relationship management ○ service design: ▪ service catalogue management ▪ service level management ▪ capacity management ▪ availability management

	▪ IT service continuity management ▪ information security management ▪ supplier management o service transition: ▪ transition planning ▪ change management ▪ asset and configuration management ▪ release and deployment management ▪ service validation ▪ change evaluation ▪ knowledge management o service operation: ▪ event management ▪ incident management ▪ request fulfilment ▪ problem management ▪ access management o continual service improvement: ▪ identify area and approach to improvement ▪ define what will be measured ▪ gather data ▪ process data ▪ analyse data and information ▪ present information ▪ implementation
K1.15	**The learner must understand the types of OS and related security functions** • types of OS: o desktop (for example Windows, macOS, Linux): ▪ focuses on the security of the end user (for example, antivirus added at desktop level) o server (for example Windows Server): ▪ shared services ▪ access control ▪ virus and threat protection ▪ back-ups o hypervisor type 1 and type 2: ▪ antivirus is added to the virtual machine ▪ manages all virtual machines • security functions of trusted operating systems: o user identification and authentication o mandatory access control (MAC) o discretionary access control (DAC) o object reuse protection o complete mediation o trusted path o intrusion detection
K1.16	**The learner must understand the concepts of cryptography and the importance of each stage of the key management lifecycle** • types of cryptography: o symmetric encryption:

	▪ protects data at rest ▪ uses one private key for encryption and decryption ▪ sender and receiver share one key ○ asymmetric encryption: ▪ multiple keys for encryption and decryption: • public key – encryption • private key – decryption ▪ protects data in motion • hashing: ○ one-way function ○ no key is used ○ hash value maps data to a fixed length ○ hash value calculated based on the plain text to be encrypted (for example a password) ○ recovered plain text is unreadable ○ utilised by OS to store passwords • encryption algorithms: ○ RSA ○ MD5 ○ ECC ○ PGP ○ Twofish ○ Diffie-Hellman ○ block cipher: ▪ Advanced Encryption Standard (AES) ▪ Triple DES ▪ Blowfish ○ stream cipher: ▪ QUAD • applications of cryptography: ○ authentication ○ time stamping ○ electronic money (for example, chip and pin) ○ blockchain ○ cryptocurrency ○ communication encryption: ▪ email ▪ social media ▪ applications ○ device encryption ○ protecting sensitive organisational data ○ securing websites • key management lifecycle stages: ○ key generation ○ key establishment ○ key storage ○ key usage ○ key revocation ○ key archival ○ key destruction

Skills – What you need to teach	
S1.1	**The learner must be able to research and analyse information of known cyber threats** • identify scope of research • identify appropriate and reputable sources of known cyber threats • investigate and interpret relevant known cyber threat information • observe performance and behaviour of digital systems • analyse and compare behaviour of digital systems against information of known cyber threats • create documentation that recommends appropriate mitigation strategies to defend against common attacks based on completed research and analysis outcomes

S1.2	**The learner must be able to design and implement systems to meet security objectives**
	
	• review security objectives requirements
	• design network component diagram to meet security objectives
	• develop encryption management plan:
	  ○ apply encryption key lifecycle
	  ○ identify encryption algorithms
	  ○ determine role-based access
	  ○ select appropriate key generator tool
	  ○ determine key management and storage options
	• implement plan to manage encryption key

Theme 2: Legislation

Knowledge – What you need to teach	

K2.1	**The learner must understand the key principles of legislation and standards applicable to the cyber engineering role**
	
	• legislation:
	  o General Data Protection Regulation (GDPR)/Data Protection Act (DPA) 2018
	  ▪ key principles:
	  • fair, lawful and transparent processing
	  • purpose limitation
	  • data minimisation
	  • accuracy
	  • storage limitation
	  • integrity and confidentiality (security)
	  • accountability
	  ▪ Data Protection Impact Assessment (DIPA)
	  o Computer Misuse Act 1990:
	  ▪ governs access offences:
	  • unauthorised access to computer materials
	  • unauthorised access with intent to commit or facilitate commission of further offences
	  • unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computers
	  • unlawful copying, adaption, supplying or obtaining of articles for use in unlawfully gaining access to computer materials or impairing the operation of a computer
	  o Copyright, Designs and Patents Act 1988:
	  ▪ key principles:
	  • rules for subsistence, ownership and copyright protection
	  • establishes rights of copyright owners
	  • establishes permitted acts
	  • governance of copyrights and infringements
	  o Intelligence Services Act 1994:
	  ▪ key principles:
	  • allows rights for intelligence and security agents to covertly monitor digital assets and activities
	  • governs hacking by agents with the aim of destroying or manipulating the function of a digital system
	  o Regulation of Investigatory Powers Act (RIPA) 2000:
	  ▪ key principles:
	  • governs public body access to customer communications
	  • enables surveillance of communication in transit
	  • surveillance of internet usage and activities
	  • enables certain public bodies to fit equipment to facilitate surveillance
	  • enables public bodies to request disclosure of protected or encrypted information
	• regulations and standards:
	  o ISO 27001:2013:
	  ▪ key principles govern:
	  • organisational context and stakeholders

	• planning information security management systems' (ISMS) risk assessment and risk mitigation • supporting information security management systems • reviewing system performance • corrective action • controls sit inside 14 groups: o A5 information security polices o A6 organisational information security o A7 human resource security o A8 asset management o A9 access control o A10 cryptography o A11 physical and environmental security o A12 operation security o A13 communication security o A14 system acquisition development and maintenance o A15 supplier relationships o A16 information security incident management o A17 information security aspects of business continuity management o A18 compliance with internal and external requirements o NCSC: ▪ Cyber Essentials: • key principles of self-assessment: o firewalls and internet gateways o secure configuration o software patching o user accounts o administrative accounts o malware protection ▪ Cyber Assessment Framework (CAF): • key objectives: o managing a security risk o protecting against cyber attack o detecting cyber security events o minimising impact of cyber security incidents o NIST: ▪ cyber security topics: • configuration and vulnerability management • cryptography • cyber security education and workforce development • risk management
K2.2	**The learner must understand the principles of security management systems** • governance: o industry and organisational: ▪ standards: • ISO 27001:2013 – ISMS standard • ISO 27002:2013 – control descriptions • ISO 27005:2018 – risk management • ISO 27701:2019 – personably identifiable information • ISO 22301:2019 – business continuity management ▪ policies: • acceptable use policy (AUP)

	• access control policy (ACP) • change management policy • information security policy • incident response policy • identity access and management policy • personal and mobile device policy • server policy • back up policy ▪ processes ▪ guidelines o organisational structure: ▪ people ▪ process ▪ technology o roles within security management: ▪ board ▪ steering committees ▪ business unit managers ▪ system owners ▪ information asset owners ▪ information asset custodians o role responsibilities to meet security outcomes: ▪ ownership: • project • risk • asset • process ▪ guidance: • internal • external (for example, managed security services partner (MSSP), consultancy) ▪ operationalisation ▪ custodianship: • process owner • procedure owner ▪ quality management: • product/service quality • compliance • audit
K2.3	**The learner must understand the NCSC 10 Steps to Cyber Security standard and its ethical application within a cyber security role** • NCSC 10 Steps: o network security: ▪ protect networks from attack ▪ defend the network perimeter ▪ filter out unauthorised access and malicious content ▪ monitor and test security controls o user education and awareness: ▪ user policies ▪ staff training ▪ maintain awareness of cyber risks

	○ home and mobile working: ▪ develop mobile working policy ▪ apply the secure baseline and build to all devices ▪ protect data in transit and at rest ○ secure configuration: ▪ apply security patches ▪ ensure secure configuration of all systems is maintained ▪ create system inventory and define baseline build for all devices ○ removable media controls: ▪ policy to control access to removable media ▪ limit media types and use ▪ scan all media for malware ○ managing user privilege: ▪ limit number of privileged accounts ▪ limit user privileges and monitor user activity ▪ control access to activity and audit logs ○ incident management: ▪ establish incident response and disaster recovery capability ▪ test incident management plans ▪ provide specialist training ▪ report criminal incidents to law enforcement ○ monitoring: ▪ establish monitoring strategy and produce supporting policies ▪ continuously monitor all systems and networks ▪ analyse logs for unusual activity that could indicate an attack ○ malware protection: ▪ produce relevant policies ▪ establish anti-malware defences across organisation

Theme 3: Threat intelligence

Knowledge – What you need to teach	

K3.1	**The learner must understand the importance of monitoring the threat landscape and trend threat analysis**
	
	• monitoring threat landscape:
	  o importance of threat trend analysis:
	  ▪ informs business strategy planning
	  ▪ enables implementation of predictive security measures
	  ▪ supports future proofing of systems
	  ▪ time saving
	  ▪ informs cost benefit analysis
	  o value and risk of threat trend analysis:
	  ▪ acting on incorrect threat intelligence:
	  • financial
	  • operational
	  • reputational
	  ▪ value of threat trend analysis:
	  • resource planning
	  • sharing national intelligence
	  • customer confidence

K3.2	**The learner must understand the components of risk management within cyber security**
	
	• stages of risk assessment within cyber security:
	  o asset identification
	  o assign asset owners
	  o assign asset classification:
	  ▪ sensitivity and criticality
	  o identification:
	  ▪ threats
	  ▪ vulnerabilities
	  o probability:
	  ▪ likelihood of occurrence
	  o impact:
	  ▪ products
	  ▪ services
	  ▪ assets
	  ▪ cost to organisation
	  o prioritisation:
	  ▪ based on analysis of probability and impact
	• role of risk owner/asset owner in risk response:
	  o plan and implement risk response
	  o monitor effectiveness of risk response
	  o record and report outcomes within organisational templates

K3.3	**The learner must understand the principles and implementation of security management systems** • key principles:

	○ a framework of policies and controls that manage security and risks across the whole organisation • implementation: ○ people: ▪ business interaction: • security enhancement • staff training ○ processes: ▪ organisational support of business objectives ▪ embedded security practices and policies ○ technology: ▪ to support achievement of business objectives • implementation of SMS: ○ standards: ▪ ISO 27001:2013 – ISMS standard ▪ ISO 27002:2013 – control descriptions ▪ ISO 27005:2018 – risk management ▪ ISO 27701:2019 – personably identifiable information ▪ ISO 22301:2019 – business continuity management
K3.4	**The learner must understand methods of vulnerability identification within organisations and organisational mitigation strategies** • methods of vulnerability identification and assurance: ○ third-party services ○ internal and external intelligence sharing initiatives: ▪ internal logs ▪ Open Web Application Security Project (OWASP) ▪ open-source intelligence (OSINT) ○ alerts from technologies ○ review of logs: ▪ software ▪ hardware ○ Wi Fi traffic analysis ○ penetration testing ○ end user notification ○ network protocol analyser ○ dark web monitoring ○ security information and event management (SIEM) tools • organisational mitigation strategies: ○ device hardening ○ patching ○ air gapping ○ multi-factor authentication ○ access control privileges ○ encryption ○ secure configuration ○ boundary firewall ○ single sign on
K3.5	**The learner must understand the purpose and stages of the threat intelligence lifecycle** • purpose of threat intelligence lifecycle: ○ horizon scanning

	○ identifies attacker ○ determines attacker's motivation ○ identifies attack methods ○ informs mitigation techniques • stages of threat intelligence lifecycle: ○ planning and direction ▪ identification of threats to assets ▪ types of threat intelligence required ▪ impact of threat ○ collection: ▪ from recognised sources of threat intelligence and vulnerabilities: • data collection from internal logs • data collection from external threat intelligence ○ processing: ▪ combination of internal and external sources of threat intelligence ▪ conversion of data into useable information: • decryption • language translation • data reduction ○ analysis and production: ▪ analysis and evaluation of threat intelligence information: • contextualisation of processed threat intelligence • considerations of patterns/insufficient data • evidence of exploit being used in live environment ▪ production of documented recommendations to outline solutions ○ dissemination and feedback: ▪ transfer of documentation of analysis and solution recommendations to appropriate stakeholder ▪ evaluation and refinement of intelligence operation

Skills – What you need to teach	
S3.1	**The learner must be able to recommend improvements based on research into future potential cyber threat trends** • identification and classification of threat • identification of vulnerabilities • assess probability of threat exploiting vulnerability • assess impact on business • examine controls/countermeasures to reduce vulnerability, probability or impact • develop metrics to measure success of control/counter measures • develop a business case for recommended option
S3.2	**The learner must be able to apply the stages of the threat intelligence lifecycle to systems or processes** • determine scope of threat through planning and direction • collect cyber threat data from relevant internal and external sources in line with organisational policy • combine and process cyber threat raw data from internal and external sources to give an enriched view of cyber threats and hazards

	• analyse and evaluate threat intelligence information • produce documented recommendations to outline appropriate mitigation strategies and techniques for dissemination as appropriate • feedback recommendations to appropriate stakeholders • operate and comply with Service Level Agreement (SLA) requirements and targets (for example, time frames)
S3.3	**The learner must be able to apply the stages of cyber security risk assessment to ensure compliance with appropriate external cyber security standards** • identify potential cyber threats and vulnerabilities within a defined context • identify risk of potential threats and vulnerabilities • determine likelihood of occurrence • assess the impact on organisation • prioritise response based on impact assessment • propose appropriate mitigation strategies • assess against and compare compliance with external cyber security standards
S3.4	**The learner must be able to gather and analyse security issue information** • gather available information about security issue from reliable sources • analyse information about security issue • identify and describe actions taken to mitigate threats, vulnerabilities and risks • identify, record and communicate residual areas of concern
S3.5	**The learner must be able to configure digital system tools and technologies** • gather information from various internal and external sources to identify configuration requirements • assess current configuration and performance of digital system tools and technologies • secure information through monitoring and analysis tools (for example, SIEM tools) • monitor digital network access • apply cyber security technologies to identify cyber security vulnerabilities and breaches • assess current intelligence information about known threats and vulnerabilities: ○ review indicators of compromise • analyse information from configuration assessment and current threat intelligence information • configure device based on optimal and secure configuration • deploy and apply appropriate digital network and cyber security technologies to meet outcome

Theme 4: Security by design

Skills – What you need to teach	

S4.1	**The learner must be able to design and build systems to meet specification requirements**
	
	• review specification requirements
	• design system components to meet specification:
	  o security hardware
	  o security software
	• configure hardware and software to meet specification
	• test and record performance of security system
	• assess test information against specification requirements

S4.2	**The learner must be able to design and build a network to meet specification requirements**
	
	• review requirements of secure network
	• design network to meet requirements:
	  o multiple subnets
	  o static and dynamic routes
	• document design
	• build network based on design
	• test network:
	  o develop test scripts against design requirement
	  o run tests
	  o troubleshoot issues
	  o document outcomes of tests
	• assess network build against design requirements
	• develop handover documentation for support

S4.3	**The learner must be able to identify, research and troubleshoot vulnerabilities and issues within systems and networks** • conduct troubleshooting to identify potential vulnerabilities and issues through practical exploration • gather threat intelligence information from practical exploration • research and compare gathered threat intelligence against known threat intelligence • explore potential mitigations and novel solutions based on research and threat intelligence • create action plan based on research and practical exploration • implement appropriate action plan to achieve outcome

S4.4	**The learner must be able to prevent breaches to digital systems**
	
	• conduct a vulnerability assessment:
	  o people
	  o processes
	  o technology
	• interpret results of vulnerability assessment
	• identify appropriate resolution to mitigate vulnerabilities
	• apply appropriate tools or techniques to mitigate vulnerabilities

	• repeat vulnerability assessment to test outcome • record actions and outcome

Theme 5: Cyber security management

Knowledge – What you need to teach	

K5.1	**The learner must understand the components of scoping and analysis of stakeholder requirements for the development of security objectives**
	
	• scoping of security objective requirements:
	  o stakeholder type:
	  ▪ executive
	  ▪ employee (for example, standard user/privileged user)
	  ▪ customer
	  o location:
	  ▪ remote
	  ▪ overseas
	  ▪ office based
	  ▪ global reach
	  ▪ global locations
	  o threats and risk identification
	  o stakeholder needs identification
	• gap analysis:
	  o current state
	  o desired future state
	  o evaluate solutions based on gap analysis

K5.2	**The learner must understand the influence of cyber security processes in incident investigation**
	
	• cyber incident response methodology:
	  o triage
	  o analyse
	  o contain or mitigate
	  o remediate or eradicate
	  o recover
	  o review
	• incident management processes:
	  o oversee
	  o communicate
	  o engage support
	  o escalate
	  o report
	  o notify
	  o lessons learned
	• digital forensics:
	  o acquisition
	  o examination
	  o analysis and reporting

Skills – What you need to teach	

S5.1	**The learner must be able to develop a security strategy**
	
	• analyse context and threat:
	  o stakeholder type
	  o location
	  o connection
	• conduct gap analysis:
	  o assess organisation's current state
	  o assess organisation's desired future state
	• evaluate options for moving from current state to desired future state:
	  o people
	  o process
	  o technology
	  o costs
	  o benefits
	  o sign off at appropriate level
	• develop plan to implement preferred option:
	  o technology requirements
	  o resource requirements
	  o timings
	  o priorities
	  o sign off at appropriate level

S5.2	**The learner must be able to analyse security requirements**
	
	• identify scope
	• analyse security requirements:
	  o identify functional and non-functional security requirements
	  o identify conflicting requirements
	• identify design requirements:
	  o usability
	  o cost
	  o size
	  o weight
	  o power
	  o heat
	  o supportability
	• select and justify appropriate solution:
	  o identify trade-offs:
	  ▪ cost and maintenance
	  ▪ risk and compliance
	  ▪ productivity and user experience

Theme 6: Systems and programming

Knowledge – What you need to teach	

K6.1	**The learner must understand the types and application of programming and scripting languages**
	
	• types of language:
	  ○ programming:
	  ▪ C#
	  ▪ C++
	  ▪ Java
	  ○ scripting:
	  ▪ PowerShell
	  ▪ Python
	  ▪ JavaScript
	  ▪ PHP
	• application of languages:
	  ○ applications
	  ○ automation
	  ○ web pages
	• coding standards and rules:
	  ○ understandable variables
	  ○ documented code
	  ○ input validations
	  ○ error handling
	  ○ version control

Skills – What you need to teach	
S6.1	**The learner must be able to write program code or scripts in accordance with coding standards** • review specification requirements • review employer's coding standards • write script or program to meet requirements and standards using appropriate language • test script or program

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).

Analyse	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.
Critically analyse	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.
Clarify	Explain the information in a clear, concise way showing depth of understanding.
Classify	Organise accurately according to specific criteria.
Collate	Collect and present information arranged in sequence or logical order which is suitable for purpose.
Compare	Examine the subjects in detail, consider and contrast similarities and differences.
Critically compare	This is a development of 'compare' where the learner considers and contrasts the positive aspects and limitations of the subject.
Consider	Think carefully and write about a problem, action or decision showing how views and opinions have been developed.
Demonstrate	Show an in-depth understanding by describing, explaining, or illustrating using examples.
Describe	Provide a broad range of detailed information about the subject or item in a logical way.
Discuss	Write a detailed account which includes contrasting perspectives.
Draw conclusions (which…)	Make a final decision or judgement based on reasons.
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. Apply current research or theories to support the evaluation.
Critically evaluate	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.
Explain	Apply reasoning to account for how something is or to show understanding of underpinning concepts. Responses could include examples to support these reasons.

Identify	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).
Justify	Give a detailed explanation of the reasons for actions or decisions.
Reflect	Learners should consider their actions, experiences or learning and the implications of these in order to suggest significant developments for practice and professional development.
Review and revise	Look back over the subject and make corrections or changes based on additional knowledge or experience.
Summarise	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:

- evidence and grading tracker
- learning resources
- qualification fact sheet

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/
- www.legislation.gov.uk/
- www.ncsc.gov.uk/
- www.nist.gov/
- www.owasp.org/
- www.cisco.com/
- 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 any learning resources available on these websites. For official NCFE endorsed learning resources please see the additional and teaching materials sections on the qualification page on the NCFE website.

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.qualhub.co.uk
(www.ncfe.org.uk)

DRAFT/Version 1.0 June 2022
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.***