



Group Award Specification for:

HNC Cyber Security

Group Award Code: GP10 15

Validation date: June 2018

Date of original publication: July 2018

Version: 05 (December 2020)

Contents

1	Introduction	1
2	Qualification structure.....	5
	2.1 Structure.....	5
3	Aims of the qualification	9
	3.1 General aims of the qualification	9
	3.2 Specific aims of the qualification.....	9
	3.3 Graded units.....	9
4	Recommended entry to the qualification.....	11
	4.1 Core Skills entry profile.....	11
5	Additional benefits of the qualification in meeting employer needs	12
	5.1 Mapping of qualification aims to units	13
	5.2 Mapping of National Occupational Standards (NOS) and/or trade body standards	14
	5.3 Mapping of Core Skills development opportunities across the qualifications.....	17
	5.4 Assessment strategy for the qualifications.....	18
6	Guidance on approaches to delivery and assessment.....	26
	6.1 Sequencing/integration of units	26
	6.2 Recognition of prior learning.....	29
	6.3 Opportunities for e-assessment.....	30
	6.4 Support materials	30
	6.5 Resource requirements	30
7	General information for centres	31
8	Glossary of terms	32
9	General information for learners	34

1 Introduction

This document was previously known as the Arrangements document. The purpose of this document is to:

- ◆ assist centres to implement, deliver and manage the qualification.
- ◆ provide a guide for new staff involved in offering the qualification.
- ◆ inform course managers teaching staff, assessors, learners, employers and HEIs of the aims and purpose of the qualification.
- ◆ provide details of the range of learners the qualification is suitable for and progression opportunities.

Rationale

The widespread use of digital technologies has revolutionised work and leisure. Digital technology is used in almost every job and people spend an increased proportion of their personal time using digital devices. While the expansion of this technology has improved productivity in the workplace and the quality of leisure time, it also presents security challenges. The digitisation of personal and business information presents new threats to individuals and organisations.

Governments, across the world, have responded to the increased threat of cyber-attack through various initiatives including:

- ◆ raising awareness of cyber threats among the general population
- ◆ improved general education in cyber resilience
- ◆ provision of specialist qualifications in cyber security
- ◆ audit of workplace skills
- ◆ estimates of future demand for cyber skills
- ◆ raising awareness of careers in cyber security
- ◆ improving the skills pipeline

In the *National Security Strategy 2016-2021* policy paper¹, first published in November 2016, the UK Government set out their plan to make Britain both secure and resilient in cyberspace. This plan aims to make the country 'confident, capable and resilient in a fast-moving digital world' promising to invest £1.9billion 'defending our systems and infrastructure, deterring our adversaries and developing a whole-society capability'. The policy paper highlights the critical skills shortage in cyber security, citing the lack of skilled teachers and cyber security specialists in the sector. Furthermore, the report also draws attention to the lack of young people entering the profession and the 'insufficient exposure to cyber and information security concepts in computing courses... and the absence of established career and training pathways into the profession'.

¹ National Security Strategy 2016-2021 HM Government
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

The Scottish Government has recognised the importance of enhancing cyber resilience in industry throughout the country and, in November 2017, published an action plan as part of its *Cyber Resilience Strategy for Scotland's Public Sector*. Following this pilot scheme, the Scottish Government plans to roll out a similar action plans for the Private Sector and the Third Sector to ensure an aligned and consistent approach to cyber security is adopted across the country.

Education has responded by providing learning and certification opportunities. Most UK universities provide degrees in data security; the school curriculum now includes aspects of cyber security in some National Qualifications. SQA introduced National Progression Awards in Cyber Security at SCQF levels 4, 5 and 6 in 2015/2016, which have been popular in Scottish schools and colleges. However, there is a gap between higher level qualifications (SCQF levels 9, 10 and 11) and lower level qualifications (SCQF levels 4, 5 and 6).

The UK's *National Security Strategy* (see above) provided funding for a range of security-related initiatives. SQA was successful in bidding for funding for two projects:

- 1 Support materials for the National Progression Awards.
- 2 Development of new intermediate level awards (SCQF levels 7, 8 and 9).

The following new qualifications were funded:

- 1 HNC Cyber Security (SCQF level 7)
- 2 HND Cyber Security (SCQF level 8)
- 3 Professional Development Awards in Cyber Security (SCQF levels 7, 8 and 9)

This qualification is the first qualification in this suite. The HND will be available from session 2019/2020. The PDAs will be available from 2020/2021.

The HNC Cyber Security will build on the National Progression Awards in Cyber Security at SCQF levels 4, 5 and 6, providing a clear progression path to SCQF level 7 (HNC) and level 8 (HND). In doing so, it will complete the skills pipeline into the cyber security industry, bridging the gap between the largely school-based NPAs and university courses, whilst sitting alongside the Diploma for Information Security Professionals. The title of the award ensures consistency between the NPAs in Cyber Security and many of the degree programmes on offer in universities, which include cyber security in their titles.

Target learner groups

The HNC Cyber Security will be suitable for a wide range of learners including:

- ◆ school leavers who wish to pursue a career in cyber security
- ◆ college learners who have completed a lower level qualification in Computing or a related field
- ◆ adults who wish to retrain in this field
- ◆ adults in employment, wishing to gain a recognised national qualification as part of Continuing Professional Development (CPD) requirements; this could be on a day-release or part-time basis.

Articulation opportunities

The HNC Cyber Security will allow progression to the HND Cyber Security (available from August 2019) and various degree programmes. Degrees related to Cyber Security currently include:

- ◆ BSc Cyber Security (University of the West of Scotland, Robert Gordon University)
- ◆ BSc Ethical Hacking (Abertay University)
- ◆ BEng Cyber Security and Forensics (Napier University)
- ◆ BSc Cyber Security and Networks (Glasgow Caledonian University)

Employment opportunities

Cyber security is a skills shortage area of strategic importance to the UK Government. Skilled staff will be required in a variety of roles, including:

- ◆ Data Protection Officer
- ◆ Ethical Hacker
- ◆ Forensics Engineer
- ◆ Information Security Architect
- ◆ Information Systems Auditor
- ◆ Penetration Tester
- ◆ Security Analyst
- ◆ Security Incident Response team member
- ◆ Security Software Developer
- ◆ Virus Technician
- ◆ Vulnerability Assessor.

The HNC Cyber Security may attract learners in employment, who wish to improve their knowledge and skills in cyber security, and full-time learners who wish to enter the security industry. The former group, depending on their existing knowledge and experience, could gain direct employment in one of these roles; the latter group, most likely, would require to progress to university in order to secure employment in this sector. The flexibility of the optional units of the qualification presents opportunities to cluster units together to form streams. Such streams could be designed to reflect particular areas of employment in the sector.

Streams could be designed around specific areas of cyber security such as:

- ◆ securing people and information
- ◆ securing networks
- ◆ programming and scripting for security

Key units in the securing people and information stream could include *Social Engineering*, *Social Media*, *Team Working in Computing* and *Work Placement*.

A securing network stream could include optional units such as *Securing Network Devices*, *Routing Technologies*, *Switching Technologies*, *Firewall Essentials*.

Finally, a programming and scripting stream would include the mandatory *Computer Programming* unit as well as options such as *Scripting for Security*, *Penetration Testing*, and *Intrusion Prevention Systems*.

These streams are suggested as examples. Individual centres can design their own 'flavour' of stream to suit their needs and resources.

2 Qualification structure

This group award is made up of **12 SQA unit credits**. **Eight credits** (64 SCQF credit points) **are mandatory**, including a graded unit of 8 SCQF credit points at SCQF level 7, and must be taken by all learners, and **4 credits are optional** (32 SCQF credit points), which are selected from the list of optional units.

A mapping of Core Skills development opportunities is available in Section 5.3.

2.1 Structure

The HNC Cyber Security qualification comprises mandatory and optional units.

Mandatory units

Learners must achieve **all** of the following eight units (8 SQA credits).

Code	Title	Level	SQA Credit	SCQF credit points	Status
J0J8 34	Computer Architecture	7	1	8	New
J0HJ 34	Computer Networking: Concepts, Practice and Introduction to Security	7	1	8	New
J0HA 34	Computer Programming	7	1	8	New
J0H9 34	Data Security	7	1	8	New
J0HL 34	Digital Forensics ²	7	1	8	Revised
J0HK 34	Ethical Hacking ³	7	1	8	Revised
J0J7 34	HNC Cyber Security: Graded Unit 1 (Examination)	7	1	8	New
J0HH 34	Professionalism and Ethics in Cyber Security	7	1	8	New

Table 1: Mandatory units

The mandatory units were selected to provide foundation knowledge and skills in cyber security. Learners may come from a wide range of backgrounds, some with no previous formal experience of computing. The mandatory units provide a wide ranging, if relatively shallow, coverage of the essential knowledge and skills required from cyber security specialists.

² Revision to H1EN 34 Computer Forensics: Fundamentals.

³ Revision to H1EP 34 Ethical Hacking: Fundamentals.

Optional units

Learners must achieve **at least 4** credits from the following optional units.

Code	Title	Level	SQA Credit	SCQF credit points	Status
HT9T 34	Artificial Intelligence	7	1	8	Existing
H8W8 34	Big Data	7	1	8	Existing
H1EM 34	Client Operating Systems	7	2	16	Existing
H179 34	Cloud Computing	7	1	8	Existing
HH3H 34	Computer Programming: Applied Mathematics	7	1	8	Existing
HT9V 34	Cyber Resilience	7	1	8	Existing
J0HG 34	Digital Forensics Case Studies	7	1	8	New
HF85 34	Emerging Technologies and Experiences	7	1	8	Existing
J2JW 34*	Firewall Essentials	7	2	16	New
J0HC 34	Internet of Things	7	1	8	New
H17M 34	Intrusion Prevention Systems	7	1	8	Existing
J0J9 34	Machine Learning	7	1	8	New
HH7W 34	Machines, Languages and Computation	7	2	16	Existing
H17R 35	Mobile Technology	8	1	8	Existing
DH3A 34	Multi User Operating Systems	7	1	8	Existing
HT9G 34	Network Security Concepts	7	2	16	Existing
FR24 35	Networking Technology	8	2	16	Existing
J0HB 34	Penetration Testing	7	1	8	New
DE3R 34	Personal Development Planning ⁴	7	1	8	Existing
H8N5 35	Private Cloud Virtualisation	8	1	8	Existing
HG1K 34	Professional Career Development in the IT Industry	7	1	8	Existing

⁴ Mandatory in all HN awards.

Code	Title	Level	SQA Credit	SCQF credit points	Status
H17D 34	Computing: Introduction to Project Management	7	1	8	Existing
FR22 35	Routing Technology	8	2	16	Existing
J0HD 34	Scripting for Security	7	1	8	New
J0HE 34	Securing Networking Devices	7	1	8	New
J0HF 34	Social Engineering	7	1	8	New
HT9W 34	Social Media	7	1	8	Existing
DH3J 34	SQL: Introduction	7	1	8	Existing
FR23 35	Switching Technology	8	2	16	Existing
H178 34	Team Working in Computing	7	1	8	Existing
H177 34	Troubleshooting Computing Problems	7	1	8	Existing
HJ4W 34	Work Placement	7	1	8	Existing
H17B 34*	Computer Networking: Practical	7	1	8	Existing
H17W 34*	Software Development: Developing Small Standalone Applications	7	2	16	Existing
J4BF 34*	Cryptography: Practical Applications	7	1	8	New
J4BG 34*	Application Security	7	1	8	New
J4BH 34*	Software Security	7	1	8	New

* Refer to History of Changes for revision changes.

Table 2: Optional units

Building units for HNC

The mandatory units of the award reflect its aims and purposes, and are the main building blocks of the award. The optional units provide subject specific learning in specific areas, such as networking, cloud computing and team working.

Computer Architecture introduces learners to the key areas of number and logic systems, as well as the workings of hardware and software elements. Such underpinning knowledge and skills will be critical for units later on in the program.

In a similar way, the *Computer Networking* unit introduces learners to IP addressing, the OSI Model, and networking protocols and services that are crucial for understanding network security issues in other units.

The inclusion of the *Computer Programming* unit as a mandatory will ensure that all learners are exposed to the principles of coding. This unit provides essential knowledge and skills that will serve as grounding for more specific subjects within the cyber security portfolio.

Professionalism and Ethics in Cyber Security introduces learners to computer-related legislation, professional bodies and the ethical impact of computing on individuals and society. Knowledge of legislation will be built on in other subjects, such as *Data Security*, where appropriate legislation is introduced.

3 Aims of the qualification

The principle aim is to have a modern and flexible qualification that will equip learners with the practical skills and knowledge to allow them to progress to higher education and/or relevant employment in the information security industry.

The aims have been categorised as 'general' or 'specific'. General aims relate to broad educational objectives; specific aims relate to the specific vocational field.

3.1 General aims of the qualification

- 1 To develop learners' knowledge and skills in the key areas of cyber security.
- 2 To develop transferrable skills required by employers and/or universities.
- 3 To encourage learners to keep up to date with fast moving emerging technologies, security threats and defence mechanisms.
- 4 To motivate and challenge learners.
- 5 To develop study and research skills.
- 6 To enhance learners' employment prospects.
- 7 To address the current national skills gap in cyber security.

3.2 Specific aims of the qualification

- 8 To prepare learners to progress to further study in cyber security in further and/or higher education.
- 9 To develop knowledge and understanding in core areas of cyber security, such as digital forensics, ethical hacking and digital security.
- 10 To develop knowledge and understanding of critical legislative considerations in cyber security for individuals and companies.
- 11 To develop learners with technical and employment skills to enhance their prospects when seeking jobs in the Cyber Security industry.
- 12 To develop an awareness of the potential impact of breaches in cyber security on individuals, companies and on society as a whole.

3.3 Graded units

Graded units assess the learner's ability to integrate and apply the knowledge and/or skills gained in the individual units in order to demonstrate that they have achieved the principal aims of the qualifications.

The graded unit may be one of two types of graded units: a project or an examination. Learners can be awarded a grade of A, B or C.

The Qualifications Development Team (QDT) selected an examination-based graded unit. An examination was chosen for several reasons, including:

- ◆ Appropriateness: An examination was selected to assess the underpinning knowledge and understanding within the award of key areas in cyber security. The qualification contains a significant body of knowledge that is best assessed by an examination.
- ◆ Consistency: Other existing HNCs, such as HNC Computing and HNC Data Analytics, follow this same type of graded unit (ie examination).

The *Graded Unit 1* examination will assess four of the mandatory units:

J0HJ 34 *Computer Networking: Concepts, Practice and Introduction to Security*

J0H9 34 *Data Security*

J0HL 34 *Digital Forensics*

J0HK 34 *Ethical Hacking*

The graded unit for this award is designed to provide evidence that the learner has achieved the following principle aims of the HNC Cyber Security:

- ◆ To develop study and research skills.
- ◆ To develop knowledge and understanding in core areas of cyber security, such as digital forensics, ethical hacking and digital security.
- ◆ To prepare learners to progress to further study in cyber security in further and/or higher education.

4 Recommended entry to the qualification

Entry to this qualification is at the discretion of the centre. The following information on prior knowledge, skills, experience or qualifications that provide suitable preparation for this qualification has been provided by the Qualification Design Team as guidance only.

Learners would benefit from having attained the skills, knowledge and understanding required by one, or more, of the following, or equivalent, qualifications and/or experience:

- ◆ National Certificate in a Computing discipline at SCQF level 5 or 6
- ◆ Any one relevant Higher (SCQF level 6) together with three National 5 courses
- ◆ Relevant National Progression Awards, such as the NPA in Cyber Security at SCQF level 5 or 6
- ◆ Relevant industrial experience

4.1 Core Skills entry profile

The Core Skill entry profile provides a summary of the associated assessment activities that exemplify why a particular level has been recommended for this qualification. The information should be used to identify if additional learning support needs to be put in place for learners whose Core Skills profile is below the recommended entry level or whether learners should be encouraged to do an alternative level or learning programme. A detailed outline of the Core Skills Development opportunities is provided in Section 5.3

Core Skill	Recommended SCQF entry profile	Associated assessment activities
Communication	5	Report and evaluation writing. Program design documentation.
Numeracy	5	Basic mathematical operation in programming. Logical operators. Binary and Hexadecimal calculations.
Information and Communication Technology (ICT)	5	Research and present information.
Problem Solving	5	Analysis, coding and testing.
Working with Others	5	Participating in the planning and organising of a group ICT project.

Table 3: Core skill profile

5 Additional benefits of the qualification in meeting employer needs

This qualification was designed to meet a specific purpose and what follows are details on how that purpose has been met through mapping of the units to the aims of the qualification. Through meeting the aims, additional value has been achieved by linking the unit standards with those defined in National Occupational Standards and/or trade/professional body requirements. In addition, significant opportunities exist for learners to develop the more generic skill, known as Core Skills through doing this qualification.

5.1 Mapping of qualification aims to units

Code	Unit title	General aims							Specific aims				
		1	2	3	4	5	6	7	8	9	10	11	12
J0J8 34	Computer Architecture	X	X	X			X	X	X			X	
J0HJ 34	Computer Networking: Concepts, Practice and Introduction to Security	X	X	X	X		X	X	X			X	
J0HA 34	Computer Programming	X	X				X	X	X	X		X	
J0H9 34	Data Security	X	X	X	X		X	X	X	X	X	X	X
J0HL 34	Digital Forensics	X	X	X	X		X	X	X	X	X	X	X
J0HK 34	Ethical Hacking			X	X				X				X
J0HH 34	Professionalism and Ethics in Cyber Security						X		X		X		X
J0J7 34	HNC Cyber Security: Graded Unit 1 (Examination)	X	X			X		X					

Table 4: Mapping of aims to units

5.2 Mapping of National Occupational Standards (NOS) and/or trade body standards

The National Occupational Standards for IT professionals are industry standards for skills, developed in collaboration with employers, professional bodies and others. They are continually updated for all key disciplines of the tech profession, and provide the building blocks for qualifications and training. The standards have been developed in line with the [Skills Framework for the Information Age \(SFIA\)](#).

The purpose of the standards is to:

- ◆ define the capabilities (performance, knowledge and understanding) required to operate as an IT professional.
- ◆ make it easier for employers to describe job roles, externally and internally.
- ◆ provide a standard taxonomy for recognising the skills levels of employees and setting development objectives.
- ◆ enable the benchmarking of degrees and training courses against employer needs.
- ◆ help training providers and educators to develop courses that meet the needs of the tech sector.
- ◆ provide guidance to regulators when accrediting qualifications.

The IT Professional Standards are organised in eight disciplines for the profession.

- 1 [Architecture, Analysis and Design](#)
- 2 [Business Change Management](#)
- 3 [Data Analytics](#)
- 4 [Information Management](#)
- 5 [Information Security \(fully updated – Apr 16\)](#)
- 6 [IT Service Management and Delivery](#)
- 7 [Networks](#)
- 8 [Solution Development and Implementation \(includes 2 new standards – Apr 16\)](#)

The categories relevant to the HNC Cyber Security are:

- ◆ Information Security (level 3)
- ◆ Networks (level 3)

Information Security	Level 3
Information Security Governance	TECIS60131 Contribute to information security governance activities
Secure Development and Security Architecture	TECIS60331 Contribute to information security architecture activities TECIS60332 Contribute to secure software development activities
Security Testing	TECIS60431 Contribute to information security testing activities
Secure Operations Management, Vulnerability Assessments, and Identity and Access Management	TECIS60531 Contribute to operational information security management activities TECIS60532 Contribute to information security vulnerability assessments TECIS60533 Contribute to information security identity and access management activities
Intrusion Detection, Incident Investigation and Management, and Digital Forensic	TECIS60631 Contribute to information security intrusion detection and analysis activities TECIS60632 Contribute to information security incident investigation and management activities TECIS60633 Contribute to digital forensic examination activities

Code	Unit title	National Occupational Standard									
		TECIS60131	TECIS60331	TECIS60332	TECIS60431	TECIS60531	TECIS60532	TECIS60533	TECIS60631	TECIS60632	TECIS60633
J0J8 34	Computer Architecture		x								x
J0HJ 34	Computer Networking: Concepts, Practice and Introduction to Security		x		x						
J0HA 34	Computer Programming			x							
J0H9 34	Data Security	x			x	x	x	x			
J0HL 34	Digital Forensics			x					x	x	x
J0HK 34	Ethical Hacking				x		x		x	x	
J0J7 34	HNC Cyber Security: Graded Unit 1 (Examination)	x	x	x	x						
J0HH 34	Professionalism and Ethics in Cyber Security	x				x		x			

Table 5: Mapping units to NOS

5.3 Mapping of Core Skills development opportunities across the qualifications

Core Skills can be delivered within an award by embedding them (in which case the award will lead to additional certification for learners' Core Skills) or signposting them (which does not lead to certification). Some Core Skills may be embedded in the units ('E' denotes 'embedding') and some units signpost certain Core Skills ('S' denotes 'signposting'). This is summarised in the table below.

Unit code	Unit title	Communication			Numeracy		ICT		Problem Solving			Working with Others	
		Written (Reading)	Written (Writing)	Oral	Using Number	Using Graphical Information	Accessing Information	Providing/Creating Information	Critical Thinking	Planning and Organising	Reviewing and Evaluating	Working Co-operatively with Others	Reviewing Co-operative Contribution
J0J8 34	Computer Architecture				S(5)								
J0HJ 34	Computer Networking: Concepts, Practice and Introduction to Security		S (5)		S(6)				S (6)	S(6)		S(6)	S(6)
J0HA 34	Computer Programming						S(6)	S(6)	S(6)	S(6)	S(6)		
J0H9 34	Data Security	S(6)	S(6)	S(6)			S(6)		S(6)	S(6)	S(6)		
J0HL 34	Digital Forensics	S(6)	S(6)	S(6)			S(6)	S(6)	S(6)	S(6)	S(6)		
J0HK 34	Ethical Hacking	S(6)	S(6)	S(6)	S(6)	S(6)	S(6)	S(6)	S(6)	S(6)	S(6)	S(5)	S(5)
J0J7 34	HNC Cyber Security: Graded Unit 1 (Examination)												
J0HH 34	Professionalism and Ethics in Cyber Security	S(6)	S(6)	S(6)									

Table 6: Mapping of units to Core Skills

5.4 Assessment strategy for the qualifications

The component units may be assessed individually or several units could be assessed holistically.

5.4.1 Unit assessment

This group award may be assessed unit by unit. Assessment Support Packs are available for all of the mandatory units and some of the optional units. The following table summarises the evidence requirements for each of the mandatory units.

Unit	Evidence requirements			
	Knowledge	Practical	Performance	Suggested assessments
Computer Architecture	X			<p>Outcomes 1 and 2 may take the form of a single test (multiple-choice would be acceptable), consisting of 20 questions (for each outcome) with a pass mark of 60%, carried out under supervised, timed, closed-book conditions. It can be carried out via an online assessment or a paper based one. In the case of an online assessment, learners should be able to use paper to write out their workings.</p> <p>A single assessment instrument consisting of short answer questions carried out under supervised, open-book conditions over an extended period may assess Outcomes 3 and 4. It can be carried out via an online assessment or a paper-based one.</p>
Computer Networking: Concepts, Practice and Introduction to Security	X	X		<p>Evidence for Outcome 1 could be in the form of a 20 multiple-choice question assessment. This assessment should be closed-book and time-limited to 60 minutes. This assessment could be carried out electronically or it could be paper-based, providing that the closed-book requirement is maintained. Successful completion will be deemed as gaining 60% of the answers correct (12 correct out of 20).</p> <p>Evidence for Outcomes 2, 3 and 4 will be product evidence. Learners will be required to show that they are able to configure the listed items within the knowledge and skills section of each outcome. This could be done using electronic submissions (Vlog,</p>

Unit	Evidence requirements			
	Knowledge	Practical	Performance	Suggested assessments
				Blog, Video, screenshots within a pro forma document) or written evidence.

Unit	Evidence requirements			
	Knowledge	Practical	Performance	Suggested assessments
Computer Programming	X	X		<p>A traditional approach to assessment would involve a test for Outcome 1 and Outcome 2 (to generate knowledge evidence), and a practical assignment for Outcome 3 and Outcome 4 (to generate practical evidence). The test could be a multiple-choice test and the practical assignment could be a programming task.</p> <p>A more contemporary approach to assessment would involve the use of a web log (blog) to record learning throughout the life of the unit. The blog would provide knowledge evidence (in the descriptions and explanations) and some (or all) product evidence.</p>
Data Security	X	X		<p>Suggestions for the knowledge evidence covering all outcomes (1 to 3) could be:</p> <p>Questioning using a variety of response types, for which the overall pass mark is 60%. The test could be split into sections with, for example, 20 selected response questions. The test could last an hour and sample all of the knowledge. In addition, as parts of the evidence require a description, extended response questions may be a better format to allow this opportunity. This test would be taken sight-unseen, in controlled and timed conditions without reference to teaching materials.</p> <p>Or</p> <p>A constructed response test comprising a number of short answer questions, marked and assessed traditionally. For example, the test may comprise of 10 questions, requiring a response comprising no</p>

Unit	Evidence requirements			
	Knowledge	Practical	Performance	Suggested assessments
				more than one or two paragraphs, selected across all three outcomes, each worth five marks, with the learner responses marked out of 50 and a pass mark of 25. If this approach is taken, it is recommended that some (or all) of the questions combine the knowledge and understanding within and across outcomes. This test would be taken sight-unseen, in controlled and timed conditions without reference to teaching materials. A suitable duration could be 60 minutes

Unit	Evidence requirements			
	Knowledge	Practical	Performance	Suggested assessments
				<p>A more contemporary approach to assessment would involve the use of a web log (blog) to record learning and researched case study examples throughout the life of the unit. The blog would provide knowledge evidence in the descriptions and explanations.</p> <p>The product evidence could take the form of a report with appendices. This report could generate evidence for all outcomes (2, 3 and 4). The report should address the given case study.</p>
Digital Forensics	X	X		<p>A traditional approach to summative assessment for Outcomes 1, 2 and 3 would be for learners to complete a holistic project-based assessment, where learners would work from a given case study/scenario. Learners would complete written research tasks (knowledge evidence) for Outcomes 1 and 2. For Outcome 3 (product evidence), learners would produce a report relating to the findings from Outcomes 1 and 2.</p> <p>A more contemporary approach to assessment would involve the use of a digital product, for example, a web log (blog), e-Portfolio or website to record learning (and the associated activities) throughout the life of the unit. The digital product would provide knowledge</p>

Unit	Evidence requirements			
	Knowledge	Practical	Performance	Suggested assessments
				evidence (in the descriptions and explanations) and product evidence (using, for example, video recordings and/or images).

Unit	Evidence requirements			Suggested assessments
	Knowledge	Practical	Performance	
Ethical Hacking	X	X	X	<p>The knowledge evidence comprises the underpinning knowledge required in Outcomes 1, 2, 3 and 4. A test may comprise:</p> <p>1 — A selected response test consisting of four options (one key) with a pass mark of 60%. The test could consist of a relatively high number of questions (30 or 40 for example), lasting an hour, which would span all of the outcomes and sample all of the knowledge statements (including at least one question for each statement).</p> <p>Or</p> <p>2 — A constructed response test comprising a number of short answer questions, marked and assessed traditionally. For example, the test may comprise of 10 questions, requiring a response of no more than one or two paragraphs. Questions would be selected across all three outcome and would each be worth five marks. Learner responses would be marked out of 50 with a pass mark of 25. If this approach is taken, it is recommended that some (or all) of the questions combine the knowledge and understanding within and across outcomes. This test would be taken, sight-unseen, in controlled and timed conditions without reference to teaching materials. A suitable duration would be 60 minutes.</p> <p>3 — A more contemporary approach to assessment would involve the use of a web log (blog) to record learning (and the associated activities) throughout the life of the unit. The blog would provide knowledge evidence (in the descriptions and explanations) and product evidence (using, for example, video recordings).</p> <p>The product evidence may be evidenced by a video or screen capture showing that all steps required for a penetration test have been carried out. This can be annotated or provided with a voiceover describing the steps taken.</p>

Unit	Evidence requirements			
	Knowledge	Practical	Performance	Suggested assessments
				<p>The performance evidence for Outcomes 2, 3 and 4 will demonstrate that correct procedures are being followed, from setting rules of engagement to reconnaissance, to finding vulnerabilities, exploiting them and identifying and implementing appropriate countermeasures.</p> <p>The product and performance evidence may be evidenced together by a report that covers the evidence requirements for Outcomes 2, 3 and 4.</p>
HNC Cyber Security: Graded Unit 1 (Examination)	X			A timed closed-book examination, lasting 3 hours — controlled and supervised conditions. The examination should provide the learner with the opportunity to produce evidence that demonstrates she/he has met the aims of the graded unit.
Professionalism and Ethics in Cyber Security	X			<p>A traditional approach to assessment would involve a test for all outcomes. The test could be a multiple-choice assessment. The test could consist of a number of selected response questions (SRQs) that assess the knowledge and understanding contained in Outcomes 1, 2 and 3. The test would be timed, closed-book and supervised. An appropriate pass mark would be set. Learners who achieve this threshold would achieve the three outcomes. The majority of questions would relate to factual recall (professional bodies relevant to cyber security); some questions would relate to deeper understanding and would require more complex types of questions.</p> <p>It is recommended, however, that the evidence for all three outcomes is gathered holistically through a project-based assessment, where learners would work from a given case study/scenario of a realistic environment that cyber professionals would be working in. The evidence could take an appropriate form, such as OneNote, wiki, blog or e-portfolio based on given case studies. However, other forms of evidence may also be acceptable if they demonstrate a good understanding of all the outcomes.</p>

Table 7: Unit assessment

5.4.2 Integrated assessment

An alternative approach to unit-by-unit assessment is to assess two or more units holistically. Integrated assessments combine the assessment of up to three units (24 SCQF credit points) in either an examination or project (these are known as 'alternative assessments').

For example, the knowledge evidence in the following units could be combined into a single examination:

- 1 *Computer Architecture*
- 2 *Computer Programming*
- 3 *Professionalism and Ethics in Cyber Security*

The product evidence for the following units could be combined into a single project:

- 1 *Data Security*
- 2 *Digital Forensics*
- 3 *Ethical Hacking*

A combined assessment consisting of mandatory and optional units could also be devised.

Successfully completing a combined assessment would satisfy the evidence requirements (for the specific type of evidence that the assessment seeks to demonstrate) in all of the component units.

It is left to centres to devise alternative assessments. It is recommended that centres seek prior verification of these assessments.

6 Guidance on approaches to delivery and assessment

The HNC Cyber Security is designed for learners who want to enter the field of cyber security or progress to an HND or degree in Cyber Security. The qualification can be delivered in a number of ways, including full-time, part-time or day-release.

This group award has been designed so that learners get a taste of the main areas in cyber security. Whilst some underpinning elements are similar to those in HNC Computing, the main content of the mandatory subjects are specific and unique enough to ensure that the HNC Cyber Security is a distinct qualification that can sit alongside the suite of computing-related HNCs. The flexibility of the optional units will allow centres to create a customised qualification built around the key concepts of cyber security, but allowing them full utilisation of their staff's skills sets.

The HNC Cyber Security builds upon the NPA Cyber Security, with the inclusion of mandatory units in *Ethical Hacking*, *Data Security* and *Digital Forensics*. The other mandatory units complement these by giving learners exposure to ethics and legislation; computer architecture; as well as programming and networking knowledge and skills.

The qualification can be delivered in a number of ways:

- ◆ Full-time
- ◆ Full-time fast-track
- ◆ Day-release
- ◆ Part-time evening

Centres could adopt the following suggested delivery methods:

- ◆ Lectures
- ◆ Tutorials
- ◆ Virtual machines for labs to allow a wide range of operating systems to be used safely
- ◆ Virtual learning environments
- ◆ Projects
- ◆ Group work
- ◆ Case studies

6.1 Sequencing/integration of units

The sequence of delivery is at the discretion of each centre, but the following recommendations may help with planning for delivery:

The four mandatory units assessed in the *Graded Unit 1* should be delivered and assessed prior to the commencement of the *Graded Unit 1*. *Data Security and Professionalism* and *Ethics in Cyber Security* should be delivered early to ensure that learners are exposed to the importance of legislation. *Computer Networking: Concepts, Practice and Introduction to Security* should also be delivered early, as basic networking knowledge and skills underpin several of the other practical units.

An example of a possible delivery schedule could be as follows, with five 'streams' of units across three academic blocks:

Stream	Block 1	Block 2	Block 3
1 'Data and Legislation'	Data Security	Professionalism and Ethics in Cyber Security	Graded Unit 1
2 'Networking'	Computer Networking	Networking Technologies	Networking Technologies
3 'Architecture and Programming'	Computer Architecture	Computer Programming	Machine Learning
4 'Hacking'	Ethical Hacking	Social Engineering	Penetration Testing
5 'Forensics'	Digital Forensics	Digital Forensics Case Studies	Scripting for Security

1 Example delivery pattern with a focus on **Data and Legislation**:

Code	Unit title	Mandatory (M) or Optional (O)	Block
J0H9 34	Data Security	M	1
J0HJ 34	Computer Networking: Concepts, Practice and Introduction to Security	M	1
J0J8 34	Computer Architecture	M	1
J0HC 34	Internet of Things	O	1
J0HH 34	Professionalism and Ethics in Cyber Security	M	2
J0HK 34	Ethical Hacking	M	2
J0HF 34	Social Engineering	O	2
HT9W 34	Social Media	O	2
J0HL 34	Digital Forensics	M	3
J0HA 34	Computer Programming	M	3
H8W8 34	Big Data	O	3
J0J7 34	Cyber Security: Graded Unit 1	M	3

2 Example delivery pattern with a focus on **Networking**:

Code	Unit title	Mandatory (M) or Optional (O)	Block
J0H9 34	Data Security	M	1
J0HJ 34	Computer Networking: Concepts, Practice and Introduction to Security	M	1
J0J8 34	Computer Architecture	M	1
J0HH 34	Professionalism and Ethics in Cyber Security	M	1
J0HL 34	Digital Forensics	M	2
J0HA 34	Computer Programming	M	2
FR24 35	Networking Technology	O	2
J0HK 34	Ethical Hacking	M	3
J0HE 34	Securing Networking Devices	O	3
J2JW 34*	Firewall Essentials	O	3
J0J7 34	Cyber Security: Graded Unit 1	M	3

3 Example delivery pattern with a focus on **Architecture and Programming**:

Code	Unit title	Mandatory (M) or Optional (O)	Block
J0J8 34	Computer Architecture	M	1
J0HJ 34	Computer Networking: Concepts, Practice and Introduction to Security	M	1
J0H9 34	Data Security	M	1
HT9T 34	Artificial Intelligence	O	1
J0HA 34	Computer Programming	M	2
J0HL 34	Digital Forensics	M	2
J0HC 34	Internet of Things	O	2
J0HH 34	Professionalism and Ethics in Cyber Security	M	2
J0HK 34	Ethical Hacking	M	3
J0J9 34	Machine Learning	O	3
J0HB 34	Penetration Testing	O	3
J0J7 34	Cyber Security: Graded Unit 1	M	3

4 Example delivery pattern with a focus on **Hacking**:

Code	Unit title	Mandatory (M) or Optional (O)	Block
J0H9 34	Data Security	M	1
J0HJ 34	Computer Networking: Concepts, Practice and Introduction to Security	M	1
J0HK 34	Ethical Hacking	M	1
J0HH 34	Professionalism and Ethics in Cyber Security	M	1
J0HL 34	Digital Forensics	M	2
J0HA 34	Computer Programming	M	2
J0J8 34	Computer Architecture	M	2
J0HF 34	Social Engineering	O	2
J0J7 34	Cyber Security: Graded Unit 1	M	3
J0HD 34	Scripting for Security	O	3
H17M 34	Intrusion Prevention Systems	O	3
J0HB 34	Penetration Testing	O	3

5 Example delivery pattern with a focus on **Forensics**:

Code	Unit title	Mandatory (M) or Optional (O)	Block
J0H9 34	Data Security	M	1
J0HJ 34	Computer Networking: Concepts, Practice and Introduction to Security	M	1
J0HL 34	Digital Forensics	M	1
H8W8 34	Big Data	O	1
J0HH 34	Professionalism and Ethics in Cyber Security	M	2
J0HA 34	Computer Programming	M	2
J0J8 34	Computer Architecture	M	2
J0HG 34	Digital Forensics Case Studies	O	2
J0HK 34	Ethical Hacking	M	3
J0HF 34	Social Engineering	O	3
J0HD 34	Scripting for Security	O	3
J0J7 34	Cyber Security: Graded Unit 1	M	3

This example delivery schedule is offered as a guide. Each centre should design their own delivery schedule based on staff skills, resources and learner groups and the optional units allow for a significant deal.

6.2 Recognition of prior learning

SQA recognises that learners gain knowledge and skills acquired through formal, non-formal and informal learning contexts.

In some instances, a full group award may be achieved through the recognition of prior learning. However, it is unlikely that a learner would have the appropriate prior learning and experience to meet all the requirements of a full group award.

The recognition of prior learning may **not** be used as a method of assessing in the following types of units and assessments:

- ◆ HN Graded Units
- ◆ Course and/or external assessments
- ◆ Other integrative assessment units (which may or not be graded)
- ◆ Certain types of assessment instruments where the standard may be compromised by not using the same assessment method outlined in the unit
- ◆ Where there is an existing requirement for a licence to practice
- ◆ Where there are specific health and safety requirements
- ◆ Where there are regulatory, professional or other statutory requirements
- ◆ Where otherwise specified in an assessment strategy

More information and guidance on the *Recognition of Prior Learning* (RPL) may be found on our website www.sqa.org.uk.

The following sub-sections outline how existing SQA Unit(s) may contribute to this group award. Additionally, they also outline how this group award may be recognised for professional and articulation purposes.

6.2.1 Articulation and/or progression

The HNC Cyber Security will allow progression to the HND Cyber Security (available from August 2019) and various degree programmes. Cyber security-related degrees currently include:

- ◆ BSc Cyber Security (University of the West of Scotland, Robert Gordon University)
- ◆ BSc Ethical Hacking (Abertay University)
- ◆ BEng Cyber Security and Forensics (Napier University)
- ◆ BSc Cyber Security and Networks (Glasgow Caledonian University)

This award has been designed to allow learners to gain a wide range of knowledge and skills in the key areas of cyber security, and should enable learners to specialise and progress to various degrees at different levels at the discretion of the universities.

Furthermore, there may be the opportunity for learners to continue onto a Modern Apprenticeship, for example, the level 8 Diploma for Information Security Professionals, which is part of the Technical Apprenticeship in Information Security.

6.3 Opportunities for e-assessment

Opportunities for e-assessment will be presented where multiple choice is the chosen method of assessment. This could be done via the centre's VLE or by utilising SQA's Solar facility. Where appropriate centres should adopt modern and innovative methods of capturing evidence.

6.4 Support materials

A **list of existing ASPs** is available to view on SQA's website.

6.5 Resource requirements

The HNC Cyber Security will require a mixture of specialist resources and a wide-ranging collection of hardware, software and support materials. As with the NPA Cyber Security, an on-going process of sharing of ideas, resources and good practice will be encouraged across centres. Additional learning and teaching materials to support the delivery of this group award may be produced by SQA in the future.

7 General information for centres

Equality and inclusion

The unit specifications making up this Group Award have been designed to ensure that there are no unnecessary barriers to learning or assessment. The individual needs of learners will be taken into account when planning learning experiences, selecting assessment methods or considering alternative evidence. Further advice can be found on our website www.sqa.org.uk/assessmentarrangements.

Internal and external verification

All instruments of assessment used within this/these qualification(s) should be internally verified, using the appropriate policy within the centre and the guidelines set by SQA. External verification will be carried out by SQA to ensure that internal assessment is within the national guidelines for these qualifications.

Further information on internal and external verification can be found in *SQA's Guide to Assessment* (www.sqa.org.uk/GuideToAssessment).

8 Glossary of terms

Embedded Core Skills: is where the assessment evidence for the unit also includes full evidence for complete Core Skill or Core Skill components. A learner successfully completing the unit will be automatically certificated for the Core Skill. (This depends on the unit having been successfully audited and validated for Core Skills certification.)

Finish date: The end of a group award's lapsing period is known as the finish date. After the finish date, the group award will no longer be live and the following applies:

- ◆ learners may not be entered for the group award
- ◆ the group award will continue to exist only as an archive record on the Awards Processing System (APS).

Graded unit: Graded units assess learners' ability to integrate what they have learned while working towards the units of the group award. Their purpose is to add value to the group award, making it more than the sum of its parts, and to encourage learners to retain and adapt their skills and knowledge.

Lapsing date: When a group award is entered into its lapsing period, the following will apply:

- ◆ the group award will be deleted from the relevant catalogue
- ◆ the group award specification will remain until the qualification reaches its finish date at which point it will be removed from SQA's website and archived
- ◆ no new centres may be approved to offer the group award
- ◆ centres should only enter learners whom they expect to complete the group award during the defined lapsing period

SQA credit value: The credit value allocated to a unit gives an indication of the contribution the unit makes to an SQA Group Award. An SQA credit value of 1 given to an SQA Unit represents approximately 40 hours of programmed learning, teaching and assessment.

SCQF: The Scottish Credit and Qualification Framework (SCQF) provides the national common framework for describing all relevant programmes of learning and qualifications in Scotland. SCQF terminology is used throughout this guide to refer to credits and levels. For further information on the SCQF visit the SCQF website at www.scqf.org.uk.

SCQF credit points: SCQF credit points provide a means of describing and comparing the amount of learning that is required to complete a qualification at a given level of the Framework. One National Unit credit is equivalent to 6 SCQF credit points. One National Unit credit at Advanced Higher and one Higher National Unit credit (irrespective of level) is equivalent to 8 SCQF credit points.

SCQF levels: The level a qualification is assigned within the framework is an indication of how hard it is to achieve. The SCQF covers 12 levels of learning. HNCs and HNDs are available at SCQF levels 7 and 8 respectively. Higher National Units will normally be at levels 6–9 and graded units will be at level 7 and 8. National Qualification Group Awards are available at SCQF levels 2–6 and will normally be made up of National Units which are available from SCQF levels 2–7.

Subject unit: Subject units contain vocational/subject content and are designed to test a specific set of knowledge and skills.

Signposted Core Skills: refers to opportunities to develop Core Skills arise in learning and teaching but are not automatically certificated.

9 General information for learners

This section will help you decide whether this is the qualification for you by explaining what the qualification is about, what you should know or be able to do before you start, what you will need to do during the qualification and opportunities for further learning and employment. The HNC Cyber Security will be suitable for a range of learners, in particular:

- ◆ School leavers who have gained at least one Higher (SCQF level 6) together with three passes at National 5.
- ◆ Further education learners who have completed a National Certificate in Computing with Digital Media at SCQF level 5 or level 6, or an equivalent qualification. Learners who had achieved the NPA Cyber Security at SCQF level 5 or 6 would be particularly suitable.
- ◆ Adults who wish to retrain in this vocational field, with a view to finding employment or changing career.
- ◆ Adults wishing to gain a recognised national qualification as part of Continuing Professional Development (CPD) requirements. This could be on a day-release or part-time basis.

By undertaking the award, you can take advantage of any arrangements that will be created to progress to the proposed HND Cyber Security and/or to any relevant University degree programs.

To achieve this group award, you must achieve a minimum of 12 SQA credits from the HNC Cyber Security framework, including all eight of the mandatory units. Three of the mandatory units: *Data Security*, *Digital Forensics* and *Ethical Hacking* are based on core Cyber Security subjects that make up the National Progression Award (NPA) at SCQF levels 4, 5 and 6. The other mandatory units include *Professionalism and Ethics in Cyber Security*, *Computer Programming*, *Computer Architecture and Networking*. Finally, included within the mandatory units is an examination — *Cyber Security: Graded Unit 1*. The *Graded Unit 1* examination will assess four of the mandatory units:

- ◆ *Computer Networking: Concepts, Practice and Introduction to Security*
- ◆ *Data Security*
- ◆ *Digital Forensics*
- ◆ *Ethical Hacking*

You will be introduced to a range of computing topics relating to computer systems and software development. You will also learn about important legislation in the *Data Security and Professionalism and Ethics in Cyber Security* units. It would be advantageous if you had some prior knowledge of computer hardware and software, as well as programming and networking skills. The optional units will offer you a more diverse range of cyber security topics, including scripting, social engineering, securing networking devices and the Internet of Things.