Group Award Specification for:
SQA Advanced Certificate in Cyber Security

Group Award code — GW2N 47

Publication date: January 2026

Version: 01

Contents

1 Introduction 2

2 Qualification structure 4

2.1 Structure 4

3 Aims of the qualification 7

3.1 General aims of the qualification 7

3.2 Specific aims of the qualification 7

3.3 Graded units 8

4 Recommended entry to the qualification 9

4.1 Core Skills entry profile 9

5 Additional benefits of the qualification in meeting employer needs 10

5.1 Mapping of qualification aims to units 11

5.2 Mapping of National Occupational Standards (NOS) and/or trade body standards 11

5.3 Mapping of Core Skills development opportunities across the qualification 15

5.4 Assessment strategy for the qualifications 19

5.4.1 Unit assessment 19

5.4.2 Integrated assessment 24

6 Guidance on approaches to delivery and assessment 25

6.1 Sequencing/integration of units 26

6.2 Recognition of prior learning 29

6.2.1 Articulation and/or progression 30

6.3 Opportunities for e-assessment 31

6.4 Supporting materials 31

6.5 Resource requirements 31

7 General information for centres 32

8 Glossary of terms 33

9 History of changes 35

10 General information for learners 36

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 higher education institutions of the aims and purpose of the qualification
- provide details of the range of learners that the qualification is suitable for and the progression opportunities

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 paper, 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'.

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 (NPAs) 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 SQA Advanced Certificate in 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 (SQA Advanced Certificate) and level 8 (SQA Advanced Diploma). 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, while 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.

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 SQA Advanced Certificate in Cyber Security qualification comprises mandatory and optional units.

Mandatory units

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

Code	Unit title	SQA credit	SCQF credit points	SCQF level
J1CE 47	Computer Architecture	1	8	7
J54F 47	Computer Networking: Concepts, Practice and Introduction to Security	1	8	7
J1CH 47	Computer Programming	1	8	7
J1S1 47	Data Security	1	8	7
J0L3 47	Digital Forensics	1	8	7
J0L2 47	Ethical Hacking	1	8	7
J9JP 47	Cyber Security: Graded Unit 1 (Examination)	1	8	7
J9JJ 47	Professionalism and Ethics in Cyber Security	1	8	7

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.

Optional units

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

Code	Unit title	SQA credit	SCQF credit points	SCQF level
J1CD 47	Artificial Intelligence	1	8	7
HR9T 47	Big Data	1	8	7
HP27 47	Client Operating Systems	2	16	7
HP1Y 47	Cloud Computing	1	8	7
J9JD 47	Computer Programming: Applied Mathematics	1	8	7
J45W 47	Cyber Resilience	1	8	7
J9JH 47	Digital Forensics Case Studies	1	8	7
J1CJ 47	Emerging Technologies and Experiences	1	8	7
J3CN 47	Firewall Essentials	2	16	7
J1CM 47	Internet of Things	1	8	7
HR8D 47	Intrusion Prevention Systems	1	8	7
J551 49	Machine Learning	1	8	7
HT08 47	Machines, Languages and Computation	2	16	7
HR8F 48	Mobile Technology	1	8	8
HR77 47	Multi User Operating Systems	1	8	7
HX00 47	Network Security Concepts	2	16	7
HP1M 48	Networking Technology	2	16	8
J7YE 47	Penetration Testing	1	8	7
HP6M 47	Personal Development Planning	1	8	7
HR9R 48	Private Cloud Virtualisation	1	8	8
HT06 47	Professional Career Development in the IT Industry	1	8	7
HP21 47	Computing: Introduction to Project Management	1	8	7
HP1J 48	Routing Technology	2	16	8
J8WC 47	Scripting for Security	1	8	7
J9JK 47	Securing Network Devices	1	8	7
J9JM 47	Social Engineering	1	8	7
J1GN 47	Social Media	1	8	7
HP2E 47	SQL: Introduction	1	8	7
HP1L 48	Switching Technology	2	16	8
HP1X 47	Team Working in Computing	1	8	7
HP1V 47	Troubleshooting Computing Problems	1	8	7
HP4X 47	Work Placement	1	8	7

Code	Unit title	SQA credit	SCQF credit points	SCQF level
HP20 47	Computer Networking: Practical	1	8	7
HP2N 47	Software Development: Developing Small Standalone Applications	2	16	7
J7YD 48	Network Security Monitoring	1	8	8
HP2P 47	Software Development: Programming Foundations	1	8	7
J550 47	Cryptography: Practical Applications	1	8	7
J54X 47	Application Security	1	8	7
J553 47	Software Security	1	8	7
J54E 47	Agile Development: Introduction	1	8	7

Building units for SQA Advanced Certificate

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 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 transferable 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 SQA Advanced Certificates, such as SQA Advanced Certificate Computing, follow this same type of graded unit (that is, examination).

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

J54F 47	Computer Networking: Concepts, Practice and Introduction to Security
J1S1 47	Data Security
J0L3 47	Digital Forensics
J0L2 47	Ethical Hacking

The graded unit for this award is designed to provide evidence that the learner has achieved the following principle aims of the SQA Advanced Certificate in 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 SQCF 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.

Core Skill	Recommended SCQF entry profile	Associated assessment activities
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.

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 more generic skills, known as Core Skills, through this qualification.

5.1 Mapping of qualification aims to units

Code	Title	General aims 1–7	Specific aims 8–12
J1CE 47	Computer Architecture	1,2,3,6,7	8,11
J54F 47	Computer Networking: Concepts, Practice and Introduction to Security	1,2,3,4,6,7	8,11
J1CH 47	Computer Programming	1,2,6,7	8,9,11
J1S1 47	Data Security	1,2,3,4,6,7	8,9,10,11,12
J0L3 47	Digital Forensics	1,2,3,4,6,7	8,9,10,11,12
J0L2 47	Ethical Hacking	3,4	8,12
J9JJ 47	Professionalism and Ethics in Cyber Security	6	8,10,12
J9JP 47	Cyber Security: Graded Unit 1 (Examination)	1,2,5,7	

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 — April 2016)
6. IT Service Management and Delivery
7. Networks
8. Solution Development and Implementation (Includes two new standards — April 2016)

The categories relevant to the SQA Advanced Certificate in Cyber Security are:

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

Information Security Level 3	**Standard**
Information Security Governance	TECIS60131 Contribute to information security governance activities
Secure Development and Security Architecture	TECIS60461 Contribute to information security architecture activities TECIS60462 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 TECIS60546 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 TECIS60646 Contribute to digital forensic examination activities

National Occupational Standard Mapping

Unit code	Unit title	National Occupational Standards (NOS) code
J1CE 47	Computer Architecture	TECIS60331
J54F 47	Computer Networking: Concepts, Practice and Introduction to Security	TECIS60331, TECIS60431
J1CH 47	Computer Programming	TECIS60332
J1S1 47	Data Security	TECIS60131, TECIS60431, TECIS60531, TECIS60532, TECIS60533
J0L3 47	Digital Forensics	TECIS60332, TECIS60631, TECIS60632, TECIS60633
J0L2 47	Ethical Hacking	TECIS60431, TECIS60532, TECIS60631, TECIS60632
J9JJ 47	Professionalism and Ethics in Cyber Security	TECIS60131, TECIS60531, TECIS60533
J9JP 47	Cyber Security: Graded Unit 1	TECIS60131, TECIS60331, TECIS60332, TECIS60431

5.3 Mapping of Core Skills development opportunities across the qualification

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 tables below.

Core Skill Communication components: Written (Reading), Written (Writing), Oral

Unit code	Unit title	Communication components
J54F 47	Computer Networking: Concepts, Practice and Introduction to Security	Written (Writing)(S5)
J1S1 47	Data Security	Written (Reading)(S6) Written (Writing)(S6) Oral(S6)
J0L3 47	Digital Forensics	Written (Reading)(S6) Written (Writing)(S6) Oral(S6)
J0L2 47	Ethical Hacking	Written (Reading)(S6) Written (Writing)(S6) Oral(S6)
J9JJ 47	Professionalism and Ethics in Cyber Security	Written (Reading)(S6) Written (Writing)(S6) Oral(S6)

Core Skill Numeracy components: Using Number, Using Graphical Information

Unit code	Unit title	Numeracy components
J1CE 47	Computer Architecture	Using Number(S5)
J54F 47	Computer Networking: Concepts, Practice and Introduction to Security	Using Number(S6)
J0L2 47	Ethical Hacking	Using Number(S6) Using Graphical Information(S6)

Core Skill Information and Communication Technology (ICT) components: Accessing Information, Providing / Creating Information

Unit code	Unit title	Information and Communication Technology (ICT) components
J1CH 47	Computer Programming	Accessing Information(S6) Providing / Creating Information(S6)
J1S1 47	Data Security	Accessing Information(E5) Providing / Creating Information(E5)
J0L3 47	Digital Forensics	Accessing Information(S6) Providing / Creating Information(S6)
J0L2 47	Ethical Hacking	Accessing Information(E5) Providing / Creating Information(S6)

Core Skill Problem Solving components: Critical Thinking, Planning and Organising, Reviewing and Evaluating

Unit code	Unit title	Problem Solving components
J1CE 47	Computer Architecture	Critical Thinking(E6)
J54F 47	Computer Networking: Concepts, Practice and Introduction to Security	Critical Thinking(E5) Planning and Organising(S6)
J1CH 47	Computer Programming	Critical Thinking(E5) Planning and Organising(S6) Reviewing and Evaluating(S6)
J1S1 47	Data Security	Critical Thinking(E5) Planning and Organising(S6) Reviewing and Evaluating(S6)
J0L3 47	Digital Forensics	Critical Thinking(E5) Planning and Organising(E5) Reviewing and Evaluating(E5)
J0L2 47	Ethical Hacking	Critical Thinking(E6) Planning and Organising(E6) Reviewing and Evaluating(E6)
J9JP 47	Cyber Security: Graded Unit 1	Critical Thinking(E6) Planning and Organising(E6) Reviewing and Evaluating(E6)

Core Skill Working with Others components: Working Co-operatively with Others, Reviewing Co-operative Contribution

Unit code	Unit title	Working with Others components
J54F 47	Computer Networking: Concepts, Practice and Introduction to Security	Working Co-operatively with Others(S6) Reviewing Co-operative Contribution(S6)
J9JG 48	Digital Forensics	Working Co-operatively with Others(S6) Reviewing Co-operative Contribution(S6)
J0L2 47	Ethical Hacking	Working Co-operatively with Others(S5) Reviewing Co-operative Contribution(S5)

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 title	Assessment evidence requirements
Computer Architecture	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. 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.
Computer Networking: Concepts, Practice and Introduction to Security	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). 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, blog, video, screenshots within a pro-forma document) or written evidence.

Unit title	Assessment evidence requirements
Computer Programming	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. 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.
Data Security	Suggestions for the knowledge evidence covering all outcomes (1 to 3) could be: 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. Or 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 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. 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

Unit title	Assessment evidence requirements
	knowledge evidence in the descriptions and explanations. 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.
Digital Forensics	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. 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 evidence (in the descriptions and explanations) and product evidence (using, for example, video recordings and/or images).
Ethical Hacking	The knowledge evidence comprises the underpinning knowledge required in outcomes 1, 2, 3 and 4. A test may comprise: 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). Or 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

Unit title	Assessment evidence requirements
	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. Or 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). 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. 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. The product and performance evidence may be evidenced together by a report that covers the evidence requirements for outcomes 2, 3 and 4.
Cyber Security: Graded Unit 1 (Examination)	A timed closed-book examination, lasting three hours — controlled and supervised conditions. The examination should provide the learner with the opportunity to produce evidence that demonstrates they have met the aims of the graded unit.
Professionalism and Ethics in Cyber Security	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

Unit title	Assessment evidence requirements
	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. 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.

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 SQA Advanced Certificate in Cyber Security is designed for learners who want to enter the field of cyber security or progress to an SQA Advanced Diploma 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. While some underpinning elements are similar to those in the SQA Advanced Certificate in Computing, the main content of the mandatory subjects are specific and unique enough to ensure that the SQA Advanced Certificate in Cyber Security is a distinct qualification that can sit alongside the suite of computing-related SQA Advanced Certificates. 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 SQA Advanced Certificate in Cyber Security builds upon the NPA in 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	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
J1S1 47	Data Security	M	1
J54F 47	Computer Networking: Concepts, Practice and Introduction to Security	M	1
J1CE 47	Computer Architecture	M	1
J1CM 47	Internet of Things	O	1
J9JJ 47	Professionalism and Ethics in Cyber Security	M	2
J0L2 47	Ethical Hacking	M	2
J9JM 47	Social Engineering	O	2
J1GN 47	Social Media	O	2
J0L3 47	Digital Forensics	M	3
J1CH 47	Computer Programming	M	3
HR9T 47	Big Data	O	3
J9JP 47	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
J1S1 47	Data Security	M	1
J54F 47	Computer Networking: Concepts, Practice and Introduction to Security	M	1
J1CE 47	Computer Architecture	M	1
J9JJ 47	Professionalism and Ethics in Cyber Security	M	1
J0L3 47	Digital Forensics	M	2
J1CH 47	Computer Programming	M	2
HP1M 48	Networking Technology	O	2
J0L2 47	Ethical Hacking	M	3
J9JK 47	Securing Networking Devices	O	3
J3CN 47*	Firewall Essentials	O	3
J9JP 47	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
J1CE 47	Computer Architecture	M	1
J54F 47	Computer Networking: Concepts, Practice and Introduction to Security	M	1
J1S1 47	Data Security	M	1
J1CD 47	Artificial Intelligence	O	1
J1CH 47	Computer Programming	M	2
J0L3 47	Digital Forensics	M	2
J0HC 47	Internet of Things	O	2
J9JJ 47	Professionalism and Ethics in Cyber Security	M	2
J0L2 47	Ethical Hacking	M	3
J1CN 47	Machine Learning	O	3
J7YE 47	Penetration Testing	O	3
J9JP 47	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
J1S1 47	Data Security	M	1
J54F 47	Computer Networking: Concepts, Practice and Introduction to Security	M	1
J0L2 47	Ethical Hacking	M	1
J9JJ 47	Professionalism and Ethics in Cyber Security	M	1
J0L3 47	Digital Forensics	M	2
J1CH 47	Computer Programming	M	2
J1CE 47	Computer Architecture	M	2
J9JM 47	Social Engineering	O	2
J9JP 47	Cyber Security: Graded Unit 1	M	3
J8WC 47	Scripting for Security	O	3

Code	Unit title	Mandatory (M) or Optional (O)	Block
HR8D 47	Intrusion Prevention Systems	O	3
J7YE 47	Penetration Testing	O	3

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

Code	Unit title	Mandatory (M) or Optional (O)	Block
J1S1 47	Data Security	M	1
J54F 47	Computer Networking: Concepts, Practice and Introduction to Security	M	1
J0L3 47	Digital Forensics	M	1
HR9T 47	Big Data	O	1
J9JJ 47	Professionalism and Ethics in Cyber Security	M	2
J1CH 47	Computer Programming	M	2
J1CE 47	Computer Architecture	M	2
J9JH 47	Digital Forensics Case Studies	O	2
J0L2 47	Ethical Hacking	M	3
J9JM 47	Social Engineering	O	3
J8WC 47	Scripting for Security	O	3
J9JP 47	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:

- SQA Advanced 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 license 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 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 SQA Advanced Certificate in Cyber Security will allow progression to the SQA Advanced Diploma in Cyber Security 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 Supporting materials

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

6.5 Resource requirements

The SQA Advanced Certificate in Cyber Security will require a mixture of specialist resources and a wide-ranging collection of hardware, software and support materials. As with the NPA in 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 these group awards 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).

8 Glossary of terms

Embedded Core Skills: 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:

- Candidates 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 candidates 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 SQA Advanced unit credit (irrespective of level) is equivalent to 8 SCQF credit points.

SCQF levels: The level a qualification assigned within the framework is an indication of how hard it is to achieve. The SCQF covers 12 levels of learning. SQA Advanced Certificates and SQA Advanced Diplomas are available at SCQF levels 7 and 8, respectively. SQA Advanced 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: These contain vocational/subject content and are designed to test a specific set of knowledge and skills.

Signposted Core Skills: These refer to opportunities to develop Core Skills in learning and teaching, but are not automatically certificated.

9 History of changes

It is anticipated that changes will take place during the life of the qualification and this section will record these changes. This document is the latest version and incorporates the changes summarised below. Centres are advised to check SQA's APS Navigator to confirm they are using the up to date qualification structure.

NOTE: Where a unit is revised by another unit:

- No new centres may be approved to offer the unit which has been revised.
- Centres should only enter learners for the unit which has been revised where they are expected to complete the unit before its finish date.

Version number	Description	Date

Acknowledgements

SQA acknowledges the valuable contribution that Scotland's colleges have made to the development of SQA Advanced Qualifications.

Further information

Call SQA's Customer Contact Centre on 44 (0) 141 500 5030 or 0475 279 1000.
Alternatively, complete our Centre Feedback Form.

10 General information for learners

This section will help you to decide whether this is the qualification for you by explaining: what the qualification is about; what you should know or what you should be able to do before you start; what you will need to do during the qualification; and opportunities for further learning and employment.

The SQA Advanced Certificate in 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 in 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 SQA Advanced Diploma in 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 SQA Advanced Certificate in 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 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.