# Group Award Specification for:
## SQA Advanced Diploma in Cyber Security

## Group Award code — GW2P 48

**Publication date: January 2026**

**Version: 01**

# Contents

# 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

**Background**

This qualification is part of a suite of awards in Cyber Security which were developed in response to a national (and international) focus on information security. The development of these awards was part of the Scottish Government's Cyber Resilience Strategy, Public Sector Action Plan, which was published in November 2017. The development of this qualification was part-funded by the Scottish Government.

This qualification builds on the SQA Advanced Certificate in Cyber Security.

The SQA Advanced Certificate award is incorporated within the SQA Advanced Diploma. Credits achieved as part of the SQA Advanced Certificate will fully contribute to this SQA Advanced Diploma.

**Rationale**

The title of the qualification was chosen for two reasons. Firstly, for consistency with the other awards in the suite, which are entitled 'Cyber Security'. Secondly, the term is widely used, and widely understood, in business and society as an umbrella term, covering the full range of information security activities.

The qualification is intended for full-time learners in colleges who wish to pursue a career in this field. The award is normally delivered over two academic sessions. However, it is possible to achieve the qualification by other means (such as part-time learning).

Most learners are expected to enter the qualification through one of the following routes:

1. Direct entry from school. Learners will possess appropriate National Qualifications.
2. Direct entry from employment or unemployment. Learners will typically possess a range of prior qualifications and experiences.

Potential entry points include: National Qualifications (school leavers), Foundation and Modern Apprenticeships (school leaver and young adults), SQA Advanced Certificate in Cyber Security (college learners) and a mixture of qualifications and work experience (adults). Section 4 (Recommended entry) provides further information about the types of qualifications and experiences expected from learners who wish to undertake this award.

Learners may progress to further education or employment. The qualification should permit learners to progress to degree courses in cyber security (or related subjects) with advanced standing. Direct entry to second or third year is possible.

A range of employment opportunities exist including the following job roles:

- IT support or security analyst
- systems administrator
- network engineer
- penetration tester
- cyber analyst or operations analyst

Learners may require a degree and/or relevant experience before they could apply for some of these positions.

There is no professional recognition for this qualification. However, the Cyber Security Generic Reference Curriculum (NATO) was used during its development and many of the defined competencies are included in the component units.

The qualification was developed in partnership with the following organisations:

- Dundee and Angus College
- Forth Valley College
- Glasgow Clyde College
- Harris Academy
- Jump Digital Ltd
- Police Scotland
- QA
- Scottish Power
- SQA
- University of Dundee
- University of Glasgow
- University of the West of Scotland
- Walker Gordon Associates Ltd
- West College Scotland

SQA would like to thank these organisations and the Scottish Government for their support during the development of this new qualification.

# 2 Qualification structure

This group award is made up of 30 SQA unit credits. 17 credits (136 SCQF credit points) are mandatory, including two graded units of 3 SQA credits (24 SCQF credit points) at SCQF levels 7 and 8, and must be taken by all learners, and 13 credits are optional (104 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 Diploma in Cyber Security qualification comprises mandatory and optional units.

**Mandatory units**

Learners must achieve all of the following 14 units (17 SQA credits).

| 4 code | 2 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 |
| J1CG | 48 | Computer Operating Systems | 2 | 16 | 8 |
| J1CH | 47 | Computer Programming | 1 | 8 | 7 |
| J1S1 | 47 | Data Security | 1 | 8 | 7 |
| J0L3 | 47 | Digital Forensics | 1 | 8 | 7 |
| J9JG | 48 | Digital Forensics | 1 | 8 | 8 |
| J0L2 | 47 | Ethical Hacking | 1 | 8 | 7 |
| J9JJ | 47 | Professionalism and Ethics in Cyber Security | 1 | 8 | 7 |
| J9JL | 48 | Server Administration for Cyber Security | 2 | 16 | 8 |
| J9JN | 48 | Wireless Device Security | 1 | 8 | 8 |
| J7LX | 47 | Working in Cyber Security | 1 | 8 | 7 |
| J9JP | 47 | Cyber Security: Graded Unit 1 | 1 | 8 | 7 |
| J9JR | 48 | Cyber Security: Graded Unit 2 | 2 | 16 | 8 |

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 13 credits from the following optional units.

| 4 code | 2 code | Unit title | SQA credit | SCQF credit points | SCQF level |
|---|---|---|---|---|---|
| J54E | 47 | Agile Development: Introduction | 1 | 8 | 7 |
| J1CD | 47 | Artificial Intelligence | 1 | 8 | 7 |

| 4 code | 2 code | Unit title | SQA credit | SCQF credit points | SCQF level |
|---|---|---|---|---|---|
| HR9T | 47 | Big Data | 1 | 8 | 7 |
| HP27 | 47 | Client Operating Systems | 2 | 16 | 7 |
| HP1Y | 47 | Cloud Computing | 1 | 8 | 7 |
| HP20 | 47 | Computer Networking: Practical | 1 | 8 | 7 |
| J9JD | 47 | Computer Programming: Applied Mathematics | 1 | 8 | 7 |
| J9JE | 48 | Computer Programming: Applied Mathematics | 1 | 8 | 8 |
| HP21 | 47 | Computing: Introduction to Project Management | 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 |
| J1CN | 47 | 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 |
| HP1J | 48 | Routing Technology | 2 | 16 | 8 |
| J8WC | 47 | Scripting for Security | 1 | 8 | 7 |
| J9JM | 47 | Social Engineering | 1 | 8 | 7 |
| J1GN | 47 | Social Media | 1 | 8 | 7 |
| HP2N | 47 | Software Development: Developing Small Scale Standalone Applications | 2 | 16 | 7 |
| HP2P | 47 | Software Development: Programming Foundations | 1 | 8 | 7 |
| HT0G | 48 | Software Development: Programming in PL/SQL | 2 | 16 | 8 |
| HP2E | 47 | SQL: Introduction | 1 | 8 | 7 |
| HP1L | 48 | Switching Technology | 2 | 16 | 8 |

| 4 code | 2 code | Unit title | SQA credit | SCQF credit points | SCQF level |
|---|---|---|---|---|---|
| HP1X | 47 | Team Working in Computing | 1 | 8 | 7 |
| HP1V | 47 | Troubleshooting Computing Problems | 1 | 8 | 7 |
| HP4X | 47 | Work Placement | 1 | 8 | 7 |
| (All the above optional units are in the SQA Advanced Certificate in Cyber Security framework) | | | | | |
| J54X | 47 | Application Security | 1 | 8 | 7 |
| J5FJ | 47 | Blockchain | 1 | 8 | 7 |
| J9J9 | 48 | Blockchain | 1 | 8 | 8 |
| J9JA | 48 | Computer Architecture | 1 | 8 | 8 |
| HT09 | 48 | Computer Networks: Administering Network Systems | 2 | 16 | 8 |
| J9JC | 48 | Computer Programming | 1 | 8 | 8 |
| J550 | 47 | Cryptography: Practical Applications | 1 | 8 | 7 |
| J9JF | 47 | Cyber Security Mathematics | 1 | 8 | 7 |
| J3CP | 47 | Data Flow | 1 | 8 | 7 |
| J8G9 | 47 | Manage Database Systems Using SQL | 1 | 8 | 7 |
| HP1H | 47 | Mathematics for Computing 1 | 1 | 8 | 7 |
| J7YD | 48 | Network Security Monitoring | 1 | 8 | 8 |
| HP34 | 48 | Open Source Operating Systems: Basic Server Administration | 1 | 8 | 8 |
| HP33 | 48 | Open Source Operating Systems: Introduction to Command Line Administration | 2 | 16 | 8 |
| HP2J | 48 | Relational Database Management Systems | 2 | 16 | 8 |
| J9JK | 47 | Securing Network Devices | 1 | 8 | 7 |
| HP2L | 48 | Software Development: Object Oriented Programming | 2 | 16 | 8 |
| J553 | 47 | Software Security | 1 | 8 | 7 |
| HT0L | 48 | Web Development: Producing a Data Driven Website | 1 | 8 | 8 |

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, programming, and open sources operating systems.

*Computer Operating Systems* builds on learners' understanding of the how various types of operating systems are installed, configured and updated to ensure users operate in a secure manner. Such underpinning knowledge and skills will be critical for

units later on in the program. In a similar way, *Digital Forensics* at level 8 builds on what learners have already covered as part of the SQA Advanced Certificate.

The inclusion of the level 8 *Computer Programming* unit will ensure that all learners are exposed to a more in-depth knowledge of coding and the associated knowledge and skills that will serve as grounding for more specific subjects within the cyber security portfolio.

*Working in Cyber Security* focuses learners on what skills and competencies may be sought by employers in the ever-growing industry of cyber security and gives a taste of what it is like in the industry, such as data analysis, monitoring, incident handling and reporting.

*Wireless Device Security* ensure that learners are familiar with many of the protocols, authentication methods and troubleshooting techniques that are used by the growing number of mobile devices and the associated security threats.

While there are no specific vendor awards included in the qualification, there will be opportunities for individual centres to embed vendor materials as a vehicle to deliver units that closely match the vendor curriculum. Furthermore, centres may wish to offer the chance for learners to gain vendor qualifications in addition to achieving the units. Past examples of this practice include the Cisco Networking Academy, the Linux Professional Institute and the Microsoft Professional program. Furthermore, companies such as Palo Alto offer training in security firewall configuration that may be used to deliver the underpinning knowledge and skills for units. Fortinet is a security company which offers several levels of free online training in cyber security so these may assist centres in their delivery too.

# 3 Aims of the qualification

The principle aim is to have a modern and flexible qualification that will equip learners with the knowledge and skills 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 a particular vocational field and may contextualise general aims in that employment sector.

## 3.1 General aims of the qualification

1. Develop academic abilities consistent with the SCQF level of the qualification.
2. Develop vocational competencies and prepare learners for employment.
3. Develop Core Skills and problem solving skills.
4. Develop a range of transferable and soft skills relevant to employment including computational thinking skills.
5. Develop study and research skills.
6. Stimulate interest in science, technology, engineering and mathematics.

## 3.2 Specific aims of the qualification

7. Develop knowledge and understanding on the principles of cyber security (SQA Advanced Certificate) that can be transferred to a range of contexts and technologies (SQA Advanced Diploma).
8. Prepare learners for progression into second year (SQA Advanced Certificate) or third year (SQA Advanced Diploma) of university in cyber-related degree courses.
9. Prepare learners for employment in a technician-level role (SQA Advanced Certificate) or specialist role (SQA Advanced Diploma).
10. Contribute towards the reduction in the national skills gap in cyber security (SQA Advanced Certificate and SQA Advanced Diploma).

SQA Advanced Certificate will provide a grounding in the principles and practice of cyber security. SQA Advanced Diploma will deepen these knowledge and skills through the application of these knowledge and skills in a range of technological contexts.

## 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 a project-based graded unit. A project was chosen for several reasons, including:

- Appropriateness: A project was selected to assess the knowledge and skills in the key areas of cyber security. Learners will be able to demonstrate what knowledge and skills they have learned across the whole qualification, putting it all together in a project that they plan, implement and review themselves.
- Consistency: Other existing SQA Advanced Diplomas, such as SQA Advanced Diploma in Computing: Networking and SQA Advanced Diploma in Computing: Technical Support, follow this same type of graded unit (that is, project).

It is recommended that the learner should have completed or be in the process of completing the following units prior to undertaking this graded unit:

- J1CE 47 Computer Architecture
- J54F 47 Computer Networking: Concepts, Practice and Introduction to Security
- J1S1 47 Data Security
- J0L2 47 Ethical Hacking
- J9JJ 47 Professionalism and Ethics in Cyber Security
- J1CH 47 Computer Programming
- J0L3 47 Digital Forensics
- J9JG 48 Digital Forensics
- J9JL 48 Server Administration for Cyber Security
- J7LX 47 Working in Cyber Security
- J9JN 48 Wireless Device Security
- J1CG 48 Computer Operating Systems

The graded unit for this award is designed to provide evidence that the learner has achieved the following principal aims of the SQA Advanced in Diploma Cyber Security:

- To develop a range of specialist knowledge and skills in cyber security.

- Where applicable, to provide learners with the underpinning knowledge and skills that may allow them to sit vendor certification examinations.
- To progress to further studies in a related discipline at SCQF level 9.
- To prepare learners for employment in the general category of cyber security or computer support.

# 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 Computing with Digital Media at SCQF level 6
- any one relevant Higher (SCQF level 6) together with three National 5 courses (SQA Advanced Certificate) or two Highers (SCQF level 6) (SQA Advanced Diploma)
- relevant National Progression Awards, such as the NPA in Cyber Security at SQCF level 6
- relevant industrial experience

Learners may gain direct entry into the second year of the SQA Advanced Diploma if they have already completed the SQA Advanced Certificate.

## 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 would be used to identify whether additional learning support needs should 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<br>• Program design documentation |
| **Numeracy** | 5 | • Basic mathematical operation in programming<br>• Logical operators<br>• 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 |

# 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

For details of the aims, see section 3.1 General aims of the qualification and section 3.2 Specific aims of the qualification.

| Unit code | Unit title | General aims 1 - 6 | Specific aims 7 - 10 |
|---|---|---|---|
| J54F 47 | Computer Networking: Concepts, Practice and Intro. to Security | 6 | 7,8,10 |
| J1CG 48 | Computer Operating Systems | | 7,8,10 |
| J1CH 47 | Computer Programming | 1,3,4,6 | 7,8,10 |
| J27J 48 | Computer Programming | 1,3,4,6 | 7,8,10 |
| J1S1 47 | Data Security | | 7,8,10 |
| J0L3 47 | Digital Forensics | 4,6 | 7,8,10 |
| J9JG 48 | Digital Forensics | 4,6 | 7,8,10 |
| H1EP 47 | Ethical Hacking | 3,6 | 7,8,10 |
| J9JJ 47 | Professionalism and Ethics in Cyber Security | 2,5 | 7,8,9,10 |
| J9JL 48 | Server Administration for Cyber Security | 6 | 7,8,10 |
| J9JN 48 | Wireless Device Security | 6 | 7,8,10 |
| J7LX 48 | Working in Cyber Security | 2,5 | 7,8,9,10 |
| J9JP 47 | Cyber Security: Graded Unit 1 (Examination) | 1,6 | 7,8,10 |
| J9JR 48 | Cyber Security: Graded Unit 2 (Project) | 1,5 | 8 |

## 5.2 Mapping of National Occupational Standards (NOS) and/or trade 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 Diploma in Cyber Security are:

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

| **Information Security Level 3** | **Standard** |
|---|---|
| Information Security Governance | TECIS60131<br>Contribute to information security governance activities |
| Secure Development and Security Architecture | TECIS60331<br>Contribute to information security architecture activities<br><br>TECIS60332<br>Contribute to secure software development activities |
| Security Testing | TECIS60431<br>Contribute to information security testing activities |
| Secure Operations Management, Vulnerability Assessments, and Identity and Access Management | TECIS60531<br>Contribute to operational information security management activities<br><br>TECIS60532<br>Contribute to information security vulnerability assessments<br><br>TECIS60533<br>Contribute to information security identity and access management activities |

| Information Security Level 3 | Standard |
|---|---|
| Intrusion Detection, Incident Investigation and Management, and Digital Forensic | TECIS60631<br>Contribute to information security intrusion detection and analysis activities<br><br>TECIS60632<br>Contribute to information security incident investigation and management activities<br><br>TECIS60633<br>Contribute to digital forensic examination activities |

**National Occupational Standards (NOS)**

| 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 |
| J27J 48 | Computer Programming | TECIS60332 |
| J1S1 47 | Data Security | TECIS60131, TECIS60431, TECIS60531, TECIS60532, TECIS60533 |
| J0L3 47 | Digital Forensics | TECIS60332, TECIS60631, TECIS60632, TECIS60633 |
| J9JG 48 | 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 |

| Unit code | Unit title | National Occupational Standards (NOS) code |
|---|---|---|
| J9JL 48 | Server Administration for Cyber Security | TECIS60131, TECIS60531, TECIS60532, TECIS60533 |
| J9JN 48 | Wireless Device Security | TECIS60331, TECIS60332, TECIS60631 |
| J7LX 47 | Working in Cyber Security | TECIS60131, TECIS60331 |
| J9JP 47 | Cyber Security: Graded Unit 1 | TECIS60131, TECIS60331, TECIS60332, TECIS60431 |
| J9JR 48 | Cyber Security: Graded Unit 2 | TECIS60131, TECIS60331, TECIS60332, TECIS60431, TECIS60531, TECIS60532, TECIS60533 |

## 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'). The numbers represent the SCQF level. This is summarised in the tables below for the units in this group award.

**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) |
| J27J 48 | Computer Programming | Written (Reading)(S6)<br>Written (Writing)(S6)<br>Oral(S6) |
| J1S1 47 | Data Security | Written (Reading)(S6)<br>Written (Writing)(S6)<br>Oral(S6) |
| J0L3 47 | Digital Forensics | Written (Reading)(S6)<br>Written (Writing)(S6)<br>Oral(S6) |
| J9JG 48 | Digital Forensics | Written (Reading)(S6)<br>Written (Writing)(S6)<br>Oral(S6) |

| Unit code | Unit title | Communication components |
|---|---|---|
| J0L2 47 | Ethical Hacking | Written (Reading)(S6)<br>Written (Writing)(S6)<br>Oral(S6) |
| J9JJ 47 | Professionalism and Ethics in Cyber Security | Written (Reading)(S6)<br>Written (Writing)(S6)<br>Oral(S6) |
| J9JL 48 | Server Administration for Cyber Security | Written (Writing)(S6)<br>Oral(S6) |
| J7LX 47 | Working in Cyber Security | Written (Reading)(S6)<br>Written (Writing)(S6)<br>Oral(S6) |
| J9JR 48 | Cyber Security: Graded Unit 2 | Written (Reading)(S6)<br>Written (Writing)(S6)<br>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)<br>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 |
|---|---|---|
| J1CG 48 | Computer Operating Systems | Providing / Creating Information(E6) |
| J1CH 47 | Computer Programming | Accessing Information(S6)<br>Providing / Creating Information(S6) |
| J27J 48 | Computer Programming | Accessing Information(S6)<br>Providing / Creating Information(S6) |
| J1S1 47 | Data Security | Accessing Information(E5)<br>Providing / Creating Information(E5) |
| J0L3 47 | Digital Forensics | Accessing Information(S6)<br>Providing / Creating Information(S6) |
| J9JG 48 | Digital Forensics | Accessing Information(S6)<br>Providing / Creating Information(S6) |
| J0L2 47 | Ethical Hacking | Accessing Information(E5)<br>Providing / Creating Information(S6) |
| J1CN 47 | Machine Learning | Providing / Creating Information(E6) |
| J9JL 48 | Server Administration for Cyber Security | Accessing Information(S6)<br>Providing / Creating Information(S6) |
| J7LX 47 | Working in Cyber Security | Accessing Information(S6)<br>Providing / Creating Information(S6) |

| Unit code | Unit title | Information and Communication Technology (ICT) components |
|---|---|---|
| J9JN 48 | Wireless Device Security | Accessing Information(S6)<br>Providing / Creating Information(S6) |
| J9JR 48 | Cyber Security: Graded Unit 2 | Accessing Information(S6)<br>Providing / Creating Information(S6) |

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

| Unit code | Unit title | Problem Solving components |
|---|---|---|
| J1GW 48 | Blockchain | Critical Thinking(E6) |
| J1CE 47 | Computer Architecture | Critical Thinking(E6) |
| J54F 47 | Computer Networking: Concepts, Practice and Introduction to Security | Critical Thinking(E5)<br>Planning and Organising(S6) |
| J1CG 48 | Computer Operating Systems | Critical Thinking(E6) |
| J1CH 47 | Computer Programming | Critical Thinking(E5)<br>Planning and Organising(S6)<br>Reviewing and Evaluating(S6) |
| J27J 48 | Computer Programming | Critical Thinking(S6)<br>Planning and Organising(S6)<br>Reviewing and Evaluating(S6) |

| Unit code | Unit title | Problem Solving components |
|---|---|---|
| J1S1 47 | Data Security | Critical Thinking(E5)<br>Planning and Organising(S6)<br>Reviewing and Evaluating(S6) |
| J0L3 47 | Digital Forensics | Critical Thinking(E5)<br>Planning and Organising(E5)<br>Reviewing and Evaluating(E5) |
| J9JG 48 | Digital Forensics | Critical Thinking(S6) |
| J0L2 47 | Ethical Hacking | Critical Thinking(E6)<br>Planning and Organising(E6)<br>Reviewing and Evaluating(E6) |
| J1CN 47 | Machine Learning | Critical Thinking(E6) |
| J9JL 48 | Server Administration for Cyber Security | Planning and Organising(E6)<br>Reviewing and Evaluating(E6) |
| J9JP 47 | Cyber Security: Graded Unit 1 | Critical Thinking(E6)<br>Planning and Organising(E6)<br>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)<br>Reviewing Co-operative Contribution(S6) |

| Unit code | Unit title | Working with Others components |
|---|---|---|
| J27J 48 | Computer Programming | Working Co-operatively with Others(S6) |
| J9JG 48 | Digital Forensics | Working Co-operatively with Others(S6)<br>Reviewing Co-operative Contribution(S6) |
| J0L2 47 | Ethical Hacking | Working Co-operatively with Others(S5)<br>Reviewing Co-operative Contribution(S5) |
| J9JL 48 | Server Administration for Cyber Security | Working Co-operatively with Others(S6) |

## 5.4 Assessment strategy for the qualification

The component units may be assessed individually or several units could be assessed holistically. 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.<br><br>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).<br><br>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 (J1CH 47) | 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.<br><br>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. |
| Computer Programming (J9JC 48) | The assessment could be a series of practical assignments that permit the learner to demonstrate their knowledge of algorithms and data structure. The resulting programs (or program segments) could be stored in a paper or digital portfolio. Given that the focus of the unit is theoretical knowledge of algorithms and data structures, there would be no need to contextualise the assignments. For example, the assignment could simply require learners to create a binary search tree (data structure) and then traverse the tree structure (algorithm). There is no need present this task in a problem solving context.<br><br>A series of assignments would generate the required evidence in the form of completed programs or program segments, stored in a portfolio. The portfolio would be assessed (on a pass/fail basis) using specific criteria. |
| Data Security | Suggestions for the knowledge evidence covering all outcomes (1 to 3) could be:<br><br>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. |

| Unit title | Assessment evidence requirements: |
|---|---|
| | Or<br><br>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.<br><br>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. 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 (J0L3 47) | 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.<br><br>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). |

| Unit title | Assessment evidence requirements: |
|---|---|
| Digital Forensics (J9JG 48) | A traditional approach to summative assessment for all outcomes would be for learners to complete a holistic collaborative project-based assessment, where learners would work in teams from a given case study/scenario. Learners would complete written research tasks (knowledge evidence) for outcomes 1 and 4. For outcomes 2 and 3 (product evidence), learners would undertake practical activity where product evidence would be based upon the output of the forensic acquisition and analysis process as well as findings.<br><br>A more contemporary approach to assessment would involve the use of a digital product, for example, a weblog (blog), e-portfolio 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). The digital product should be assessed using defined criteria to permit a correct judgement about the quality of the digital evidence. In this scenario, every knowledge and skill must be evidenced; sampling would not be appropriate. |
| Ethical Hacking | The knowledge evidence comprises the underpinning knowledge required in outcomes 1, 2, 3 and 4. A test may comprise:<br><br>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).<br><br>Or<br><br>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 |

| Unit title | Assessment evidence requirements: |
|---|---|
| | 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.<br><br>Or<br><br>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).<br><br>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.<br><br>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.<br><br>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. |

| Unit title | Assessment evidence requirements: |
|---|---|
| Cyber Security: Graded Unit 2 (Project) | This graded unit will be assessed by the use of a project-based practical assignment developed by centres. The practical assignment will be based on the development of a solution for a real client or on a scenario supplied by the centre. The project brief/scenario will require each learner to produce a cyber-security related project to meet the needs of the project brief. |
| 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 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.<br><br>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. |
| Server Administration for Cyber Security | A single assessment activity is recommended to cover all outcomes. The instrument of activity could be a practical assignment which would define what was expected from the learner (the design, implementation and management of a secure server infrastructure). This could be in the form of a project that learners would create given a project brief, or it could be in the form of a report which demonstrates and evidences all the learning outcomes being met. |

| Unit title | Assessment evidence requirements: |
|---|---|
| | 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 blog should be assessed using defined criteria to permit a correct judgement about the quality of the digital evidence. In this scenario, every knowledge and skill must be evidenced; sampling would not be appropriate. |
| Working in Cyber Security | Learners may be assessed using different methods, for example:<br>A constructed response test comprising several 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 four outcomes and would each be worth five marks. Learner responses would be marked out of 50 with a pass mark of 30. If this approach is taken, it is recommended that some (or all) of the questions combine the knowledge and understanding within and across the 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.<br>Case study where a brief/scenario can be provided<br>Report/presentation (individual or group)<br>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). The blog should be assessed using defined criteria to permit a correct judgement about the quality of the digital evidence. In this scenario, every knowledge and skill must be evidenced; sampling would not be appropriate. |

| Unit title | Assessment evidence requirements: |
|---|---|
| Wireless Device Security | The knowledge evidence for outcomes 1–3 could be assessed by either of the two models:<br><br>A selected response test under closed-book conditions, 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).<br><br>A closed-book, 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 1 to 3. This test would be taken, sight-unseen, in controlled and timed conditions without reference to teaching materials. A suitable duration could be 60 minutes.<br><br>The practical assignment for outcome 3 might be carried out by one assessment where an insecure wireless network has been set up and the learner is given a specification of the security issues that are to be mitigated. These should include Wireless Intrusion Detection Systems (WIDS), Wired network port security, Creation of a wireless network for personal or untrusted devices and disabling of unneeded wireless networks and Virtual Private Networks (VPN). |

# 6 Guidance on approaches to delivery and assessment

The SQA Advanced Diploma in Cyber Security is designed for learners who want to progress on from their SQA Advanced Certificate in Cyber Security and to then enter the field of cyber security or progress to a 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. 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 Diploma in Cyber Security builds upon the SQA Advanced Certificate in Cyber Security, with the inclusion of mandatory units in *Digital Forensics* at level 8, *Wireless Device Security, Server Administration for Cyber Security* and *Computer Operating Systems*.

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:

**Year 1 — SQA Advanced Certificate**

The four mandatory units assessed in *Cyber Security: Graded Unit 1* should be delivered and assessed prior to the commencement of *Cyber Security: 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 |
| J0HC 47 | Internet of Things | O | 1 |
| J9JJ 47 | Professionalism and Ethics in Cyber Security | M | 2 |
| J0L2 47 | Ethical Hacking | M | 2 |
| J0HF 47 | Social Engineering | O | 2 |
| HT9W 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 |
| FR24 48 | Networking Technology | O | 2 |
| J0L2 47 | Ethical Hacking | M | 3 |
| J0HE 47 | Securing Networking Devices | O | 3 |
| J2JW 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 |
| J0J9 47 | Machine Learning | O | 3 |
| J0HB 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 |
| J0HF 47 | Social Engineering | O | 2 |
| J9JP 47 | Cyber Security: Graded Unit 1 | M | 3 |
| J0HD 47 | Scripting for Security | O | 3 |
| H17M 47 | Intrusion Prevention Systems | O | 3 |
| J0HB 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 |
| J0HG 47 | Digital Forensics Case Studies | O | 2 |
| J0L2 47 | Ethical Hacking | M | 3 |
| J0HF 47 | Social Engineering | O | 3 |
| J0HD 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.

**Year 2 — SQA Advanced Diploma**

The three mandatory units assessed in Cyber Security: Graded Unit 2, Digital Forensics (level 8), Server Administration for Cyber Security, and Computer Operating Systems, should be delivered and assessed prior to the commencement of Cyber Security: Graded Unit 2.

In the group award structure for the SQA Advanced Certificate in Cyber Security, there were examples of a possible delivery schedule, with five ‘streams’ of units across three academic blocks. Due to the flexibility of the optional units such a delivery could be continued on to the SQA Advanced Diploma with careful curriculum and resources planning.

It may be desirable to deliver the *Computer Programming* (SCQF level 8) and *Digital Forensics* (SCQF level 8) units early in the academic year as these will build on the level 7 units learners have achieved in the SQA Advanced Certificate so the knowledge and skills would be fresh in their minds. Furthermore, centres may wish to deliver the *Working in Cyber Security* unit at the end of the academic term as learners may be starting to plan for entering the workplace at this point and such a unit would help prepare them with the skills required to do so.

There may be potential for centres to cluster units to allow a holistic approach to assessment. A similar approach to the five themed streams above could be adopted.

An obvious group of units that could be assessed together is *Cyber Security: Graded Unit 2* (project-based) along with *Server Administration for Cyber Security* and other mandatory units.

In terms of network-based units, there will be a lot of crossover between *Routing Technology* and *Switching Technology* as there are many common commands that are used to configure both routers and switches. Furthermore, the *Firewall Essentials* unit could be bolted on to the delivery of these units to complete a holistic teaching and assessment stream.

Furthermore, obvious groupings of units for holistic teaching and assessment exist in the open sources optional units as well as in the other areas of programming and forensics.

## 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-section outlines how this group award may be recognised for professional and articulation purposes.

### 6.2.1 Articulation and/or progression

The SQA Advanced Diploma in Cyber Security may allow progression to 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 an apprenticeship, for example, the level 8 Diploma for Information Security Professionals, which is part of the Technical Apprenticeship in Information Security.

### 6.2.2 Professional recognition

There is no professional recognition for this qualification. However, the Cyber Security Generic Reference Curriculum (NATO) was used during its development and many of the defined competencies are included in the component units.

### 6.2.3 Credit transfer arrangements

When new group awards are introduced, learners often wish to transfer between the old and the new frameworks. For example, they may have started on an SQA Advanced Certificate under an older framework and wish to complete their SQA Advanced Diploma on the new framework, or they may have completed units some time ago and wish to use these as part of an SQA Advanced Certificate or SQA Advanced Diploma under the new framework.

To assist in this process, SQA normally provides centres with guidance on credit transfer between the old and the new frameworks. SQA has clear criteria for deciding if two syllabuses are equivalent. All the following criteria must be satisfied if full credit transfer is to be recognised between both syllabuses:

1. The syllabuses have the same SCQF levels.
2. The syllabuses have the similar credit values (or equivalent).
3. The syllabuses are equivalent in terms of Core Skill coverage.
4. The syllabuses relate to the same subject area and the main topics are common to both.
5. The syllabuses present a similar level of cognitive demand.
6. The syllabuses encompass similar skill-sets.
7. The syllabuses are contemporary in terms of terminology, techniques and technology.
8. Employers, admission officers and other users would perceive both syllabuses as broadly equivalent.
9. The assessment demands are similar in terms of candidate activity and Performance Criteria, or candidates would be equally likely to pass both assessments.
10. Special conditions (where they exist) are applicable to both syllabuses.

## 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 exiting ASPs is available to view on SQA's website.

## 6.5 Resource requirements

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

The SQA Advanced Diploma in Cyber Security also requires a significant commitment from centres to provide an IT infrastructure that facilitates and supports learners undertaking this qualification and also the staff who deliver it. It may be necessary for centres to seek additional financial and technical support from management and from IT departments to ensure the qualification is provided with the resources it requires.

Every centre will have a different infrastructure and support structure so it would be impossible to provide a prescriptive list of what is required. However, some obvious requirements would include high performance PCs with large disk spaces for storing virtual images and also high RAM memory capacity to facilitate the running of numerous virtual machines at one time. Furthermore, as a minimum some wireless routing devices and wireless access points and network cards would be required. A variety of operating systems would be required to be available on a mixture of media (such as DVDs, memory sticks, virtual images, ISO files). Operating systems may be available to centres through licensing agreements or subscriptions to vendors but some free, open source operating systems can also be downloaded when required. Indeed, the Kali Linux

download provides a complete suite of cyber security tools that can be utilised when installed either on local machines or as virtual machines.

The creation of an isolated lab that allows only internal network traffic within the room would greatly reduce the possibility of external network issues or attacks, whether deliberate or not. Furthermore an isolated, dedicated ISP internet connection may allow the lab access to the internet without compromising the larger network infrastructure and web access of the centre.

Some of the content in the qualification such as hacking or penetration testing may also cause a level of anxiety in IT departments. Centres may wish to warn learners at the beginning of the course about acceptable behaviour and may wish to get learners to sign an acceptable usage agreement or document of understanding.

While such overheads and additional tasks may be seen as a burden, it is important to stress that because the qualification may bring some elements of risk. It is imperative to ensure that learners are aware of the risks at an early stage and are made aware of the ethical considerations that must be made to inform their actions.

# 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 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 Connect to confirm that they are using the most 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 candidates 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 0345 279 1000. Alternatively, complete our Centre Feedback Form.

# 10 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 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 and the SQA Advanced Diploma in Cyber Security provide intermediate qualifications in the field of cyber security. No previous knowledge or experience of cyber security is required but you will require qualifications and/or work experience before commencing this qualification.

The SQA Advanced Certificate is normally undertaken over one academic session. The SQA Advanced Diploma normally takes two academic sessions. Part-time delivery will take longer.

The aim of the qualifications is to prepare you for a career in cyber security. You may progress directly to employment or progress to university before employment. You could progress to the second year of university with the SQA Advanced Certificate and the third year with the SQA Advanced Diploma.

The qualifications may lead to a range of jobs including:

- technician-level post in cyber or network security
- security testing
- software testing
- programming position

The qualification includes a range of topics including:

- Data security
- Ethical hacking
- Computer networking
- Computer programming

SQA Advanced Diploma

- Digital forensics
- Artificial intelligence and big data
- Blockchain
- Internet of things

The SQA Advanced Diploma qualification, being longer than the SQA Advanced Certificate, will cover more of these topics. There may be an opportunity to undertake a work placement.

In addition to these specialist skills, you will also develop a range of Core Skills and employment skills.

You will be assessed in a variety of ways including: short tests of your knowledge, practical assignments and project work. One part of each qualification is graded, which will provide an opportunity to differentiate yourself from other learners.