Group Award Specification for:

National Progression Award (NPA) in Cyber Security at SCQF level 4

Group Award Code: GK7W 44

National Progression Award (NPA) in Cyber Security at SCQF level 5

Group Award Code: GK7X 45

National Progression Award (NPA) in Cyber Security at SCQF level 6

Group Award Code: GK7Y 46

Validation date: July 2015

Date of original publication: August 2015

Version: 01

Contents

1 Introduction

This document was previously known as the **Arrangements** document.

The purpose of this document is to:

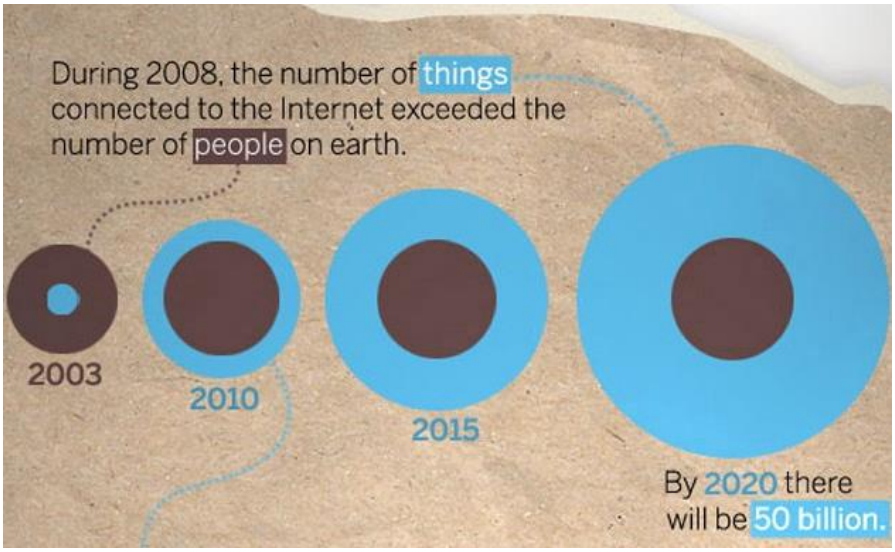
- assist centres to implement, deliver and manage the qualification
- provide a guide for new staff involved in offering the qualification
- inform course managers, teaching staff, assessors, learners, employers and HEIs of the aims and purpose of the qualification
- provide details of the range of learners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

This document describes the **rationale** for the award(s), the **structure** of the award(s), the **aims** of the award(s), the **entry** to the award(s), and any **additional benefits** from undertaking the award(s).

Rationale

As a society we conduct much of our lives over the Internet, as do the Government, the Armed Services, Law Enforcement and industry. The internet brings numerous blessings for society and for business, but it has a darker side as a refuge, resource and recruitment tool for terrorists and criminals. The UK Government takes these risks seriously. That is why the 2010 National Security Strategy rated cyber-attacks as a 'Tier 1' threat and why, despite a tight fiscal situation, the Government set £650 million aside over four years to develop their response.

It was revealed at the Digital Skills committee meeting in the House of Lords that in 2017 there will be a **global shortage of two million cyber security workers**. This increase of the need for Cyber Security Professionals is due to our reliance on devices connected to the Internet. Stephanie Doman CEO of the Cyber Security Challenge said 'if you look at our lifestyle these days everything we do is based on something connected to the internet'. Citing *Internet Banking, Shopping and Tax.*



Cost savings for governments as a result of using online services instead of telephone or face-to-face services are substantial. The creation of a common ICT infrastructure for Government will save £460 million in 2014/2015.

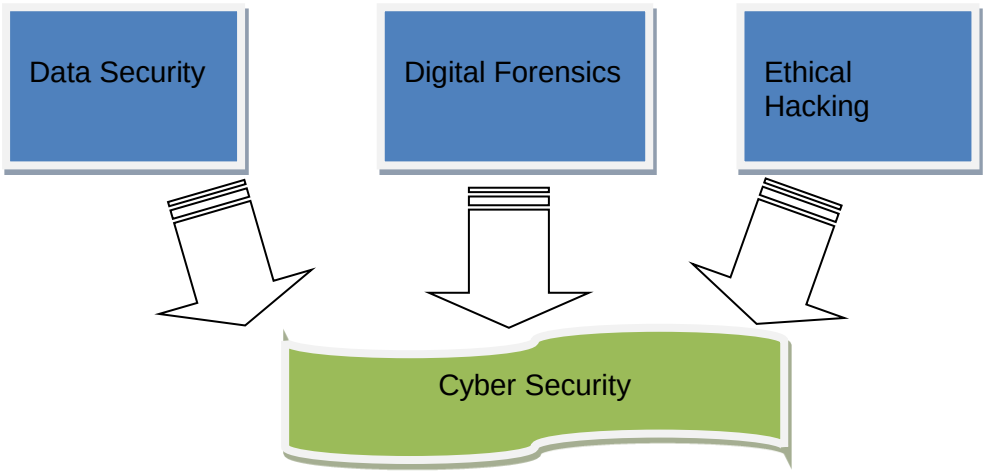
The *Department for Work and Pensions* estimates that Universal Credit will provide support to around 19 million citizens across 8.5 million households, and will include provision of online access to benefit-related services and information. Online delivery and greater automation of processes will contribute towards £500 million savings in costs, per year, once Universal Credit is fully operational.

As the Government relies more and more on online delivery and greater automation of services to save money and reduce the deficit, it is vital that the people who will access these government services and the employees that administer them have the knowledge, skills and basic cyber hygiene to protect the infrastructure.

Protecting the United Kingdom from the threat of cyber-attacks has been left to a few highly skilled and dedicated public sector and private sector cyber security professionals. This pool of professionals must grow. Only 0.6% of graduates in (2012-2013) are currently working in cyber security. Cyber security offers an innovative and exciting way of attracting talented individuals to take up rewarding careers in this field. These statistics strengthen the belief held by many industry experts that Education is key to addressing the skills gap. The proposed award has stemmed from the belief and the need to address the growing rise in easily preventable cybercrime.

The National Units within the award are designed to incorporate the three main areas of cyber security. These are:

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



This focus stems from the recognition that cyber security is essential for the success of the virtual economy, education and community and acknowledges the idea that developing the capability to understand the fundamental tools and techniques of Data Security, Digital forensics and Ethical Hacking is important in ensuring that learners are aware of their responsibilities within these virtual communities.

The National Progression Awards in Cyber Security at SCQF levels 4, 5 and 6 represent an additional, essential, vocational qualification at each level providing a clear progressive context and structure for the development of key contemporary knowledge and skills.

A key rationale for the awards is to provide a **skills pipeline** into the industry. It is anticipated that there will be significant interest in these awards within schools, and this will increase the awareness of the knowledge, skills and job opportunities required by the cyber security industry. By doing this, it is hoped that some learners will progress from these awards onto further studies in this area and, ultimately, into a career in cyber security.

These awards are the first school-based national qualification in cyber security to be developed in the EU. There is currently provision at university level in several countries (including Scotland) but, to date, nothing designed for delivery in the school sector.

The range of learners the qualification is suitable for

The qualification is suitable for a wide range of learners:

- for learners wishing to develop and enhance Cyber skills to support their learning across a wide range of curricular areas.
- for S4 to S6 school pupils who will undertake the qualification as a broadening of the Computing Science curriculum.
- for students at colleges who will be using the NPAs within full or part-time college programmes such as part of a NC Computing qualification.
- for adults returning to education with an interest in developing fundamental skills relevant to accessing a career in cyber security.

Relevance for employment opportunities

There is a current skills shortage in this area. This skills shortage will get significantly worse in the coming years, when demand for expertise in this field will far outstrip supply resulting in a global skills shortage of two million people by 2017.

It is not anticipated that these awards will lead directly to employment. They are primarily designed as ‘feeder’ qualifications to more advanced awards. By capturing the interests and imaginations of young people at a formative stage in their lives (aged 15–18), it is hoped that some will progress to further studies in this field.

However, the awards will deliver foundation knowledge and skills in cyber security that would give learners a head start if/when they progress to more advanced qualifications.

Ethical and legislative considerations

Ethics and the law are fundamental aspects of these awards. Ethical considerations are included in **every** component Unit, and legislative considerations are included in all appropriate Units.

The aim of the awards is to produce knowledgeable and skilled individuals who are aware of the potential misuses of, and unauthorised access to, computer systems but who use these competences for legal and ethical purposes.

There is specific sensitivity surrounding the illegal access to computer systems ('hacking') and particular care has been taken in the Ethical Hacking Units to emphasise that the knowledge and skills acquired must be used to defend computer systems from malicious attacks.

2 Qualifications structure

2.1 Structure

The award is available at **SCQF levels 4, 5 and 6**. Each award has the **same structure** across the levels.

Each award consists of **three** mandatory Units. There are **no** optional Units.

The total credit value of each award is **3 SQA credits** (18 SCQF credit points.).

The following tables define the award at each level.

National Progression Award in Cyber Security at SCQF level 4

4 code	2 code	Unit title	SCQF level	SCQF credit points	SQA credit
H9E2	44	Data Security	4	6	1
H9J0	44	Digital Forensics	4	6	1
H9HY	44	Ethical Hacking	4	6	1

National Progression Award in Cyber Security at SCQF level 5

4 code	2 code	Unit title	SCQF level	SCQF credit points	SQA credit
H9E2	45	Data Security	5	6	1
H9J0	45	Digital Forensics	5	6	1
H9HY	45	Ethical Hacking	5	6	1

National Progression Award in Cyber Security at SCQF level 6

4 code	2 code	Unit title	SCQF level	SCQF credit points	SQA credit
H9E2	46	Data Security	6	6	1
H9J0	46	Digital Forensics	6	6	1
H9HY	46	Ethical Hacking	6	6	1

Because of the nature of the broad-based mandatory Units, there is no requirement for optional Units. The mandatory Units span the full skillset encompassed by cyber security, comprising the essential aspects of the field.

The size of the awards (three National Units, involving **120 hours** of teaching time) fits well into school and college timetables, and has proven popular with similar awards in the past.

The awards will be placed into a **hierarchy**, which permits learners to mix-and-match Units and still gain a Group Award (at the Level of the lowest Unit). For example, if a learner undertakes the level 5 award but can only pass the *Ethical Hacking* Unit at level 4 then s/he would gain the Group Award at level 4.

Hierarchies facilitate mixed ability classes, and permit learners to gain the level of award which they are capable of achieving.

The progression through SCQF levels 4, 5 and 6 is accomplished by increasing the:

- **amount** of content (higher levels may contain new topics)
- **scope** of content (higher levels may expand the content of lower levels)
- **complexity** of content (higher levels may study the content in more complex ways)

3 Aims of the qualifications

The qualification aims to provide **foundation knowledge and skills** in cyber security to **foster an interest** in this area with the hope of **increasing the number of people choosing this field as a future career path**.

The overarching aim of the awards is to **improve the skills pipeline** in cyber security so that more young people consider a career in this area of skills shortage.

3.1 General aims of the qualifications

Each qualification aims to provide:

1 Structured contexts in which to develop knowledge and skills relevant to the use of Data Security, Digital Forensics and Ethical Hacking.
2 Opportunities to deepen knowledge and practical experience of use in personal, educational, business and community contexts.
3 Opportunities in which to develop key cognitive skills such as problem solving, analysis and evaluation.
4 Opportunities to develop collaborative skills.
5 Opportunities to develop employment skills related to National Occupational Standards.

3.2 Specific aims of the qualifications

6 To address the current national skills gap in cyber security.
7 To enable learners to contribute to safer virtual communities.
8 To develop the next generation of cyber security professionals.
9 To enable leaners to identify security weakness safely, legally and ethically.
10 To encourage new learners to have better cyber hygiene.
11 To develop cyber security skills to underpin employment.
12 To prepare learners for further study by developing cyber security skills.
13 To make learners aware of the ethical, legislative and professional factors that must be considered when dealing with cyber security.

4 Recommended entry to the qualifications

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.

Each of the awards may be undertaken without prior knowledge of cyber security. For example, there is no requirement that learners must have passed the level 4 award before attempting the level 5 award. However, learners entering the qualification hierarchy at a level above level 4 should possess a certain level of general education, which is described below.

There are a number of formal and informal qualifications that would help to prepare learners for these qualifications. This includes:

Police Scotland Cyber Security Badge
Cyber Security Fundamentals Unit at SCQF level 4
National 4/5 and Higher Computing Science

While possession of one or more of these qualifications would be advantageous to learners, they are not prerequisites.

4.1 Core Skills entry profile

Learners are required to have a certain level of general education to have a realistic prospect of succeeding in any of the awards.

The level of general education required for entry to each Level is illustrated in the table below. The table defines the level of Core Skill required for entry to any one of the three levels of this qualification.

Core Skill	**NPA level 4**	**NPA level 5**	**NPA level 6**
Communication	SCQF 3	SCQF 4	SCQF 5
Numeracy	SCQF 4	SCQF 4	SCQF 4
Information and Communication Technology	SCQF 4	SCQF 5	SCQF 6
Problem Solving	SCQF 4	SCQF 5	SCQF 5
Working with Others	SCQF 3	SCQF 4	SCQF 4

Please note that this is for guidance only. Entry to these awards is at the discretion of the centre.

5 Additional benefits of the qualification in meeting employer needs

This qualification was designed to meet a specific purpose and what follows are details on how that purpose has been met through mapping of the Units to the aims of the qualification.

Through meeting the aims, additional value has been achieved by linking the Unit standards with those defined in National Occupational Standards and/or trade/professional body requirements. In addition, significant opportunities exist for learners to develop the more generic skill, known as Core Skills through doing this qualification.

5.1 Mapping of qualification aims to Units

Code	Unit title	Aims												
		1	2	3	4	5	6	7	8	9	10	11	12	13
H9E2 44	Data Security (SCQF level 4)	X	X	X	X	X	X	X	X	X	X	X	X	X
H9J0 44	Digital Forensics (SCQF level 4)	X	X	X		X	X		X			X	X	X
H9HY 44	Ethical Hacking (SCQF level 4)	X	X	X		X	X	X	X	X		X	X	X
H9E2 45	Data Security (SCQF level 5)	X	X	X	X	X	X	X	X	X	X	X	X	X
H9J0 45	Digital Forensics (SCQF level 5)	X	X	X		X	X		X			X	X	X
H9HY 45	Ethical Hacking (SCQF level 5)	X	X	X		X	X	X	X	X		X	X	X
H9E2 46	Data Security (SCQF level 6)	X	X	X	X	X	X	X	X	X	X	X	X	X
H9J0 46	Digital Forensics (SCQF level 6)	X	X	X		X	X		X			X	X	X
H9HY 46	Ethical Hacking (SCQF level 6)	X	X	X		X	X	X	X	X		X	X	X

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

Code	Unit title	National Occupational Standard																			
		6012.01	6013.01	6013.02	6023.01	6033.01	6033.02	6043.01	6043.02	6053.01	6053.02	6063.01	6063.02	6063.03	6073.01	6073.02	6073.03	6083.01	6092.01	6092.02	6093. 01	6093.02
H9E2 44	Data Security (SCQF level 4)																					
H9J0 44	Digital Forensics (SCQF level 4)																X		X			
H9HY 44	Ethical Hacking (SCQF level 4)																					
H9E2 45	Data Security (SCQF level 5)															X				X		
H9J0 45	Digital Forensics (SCQF level 5)	X					X												X			
H9HY 45	Ethical Hacking (SCQF level 5)									X												
H9E2 46	Data Security (SCQF level 6)		X		X	X	X	X	X			X						X			X	X
H9J0 46	Digital Forensics (SCQF level 6)		X	X	X	X	X	X	X		X	X	X		X	X	X				X	X
H9HY 46	Ethical Hacking (SCQF level 6)		X		X	X	X	X	X	X	X	X	X	X	X	X	X					

Information Management		
Level 2	6012.01	Carry out specified information management activities
Level 3	6013.01	Contribute to information management
	6013.02	Document information assets
Information Governance		
Level 3	6023.01	Follow information security governance under supervision
Risk Assessment and Management		
Level 3	6033.01	Contribute to risk assessment activities, under supervision
	6033.02	Assist risk management under direction
Secure Development and Security Architecture		
Level 3	6043.01	Assist secure development, under supervision
	6043.02	Assist design of security architecture under supervision
Information Security Testing and Information Assurance Methodologies		
Level 3	6053.01	Assist security testing, under supervision
	6053.02	Assist information assurance, under supervision
Secure operations management, Service Delivery and Vulnerability Assessment		
Level 3	6063.01	Assist secure operations management activities under supervision
	6063.02	Assist secure operations under supervision
	6063.03	Assist conducting vulnerability assessments under supervision
Incident Management, Investigation and Digital Forensics		
Level 3	6073.01	Assist with incident management activities under supervision
	6073.02	Assist with incident investigation activities under supervision
	6073.03	Assist with forensic examination under supervision
Information security audit		
Level 3	6083.01	Assist in information security audit activities under supervision
IT Disaster Recovery		
Level 2	6092.01	Carry out specified IT disaster recovery activities
	6092.02	Document specified information relating to IT disaster recovery
Level 3	6093.01	Contribute to IT disaster recovery management
	6093.02	Assist with IT disaster recovery activities

5.3 Mapping of Core Skills development opportunities across the qualifications

The following table shows where each of the Units can contribute to Core Skills.

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).

None of the Core Skills are embedded within any of these awards.

However, some Units signpost certain Core Skills. This is summarised in the table below ('S' denotes 'signposting').

Unit code	Unit title	Communication		Numeracy		ICT		Problem Solving			Working with Others	
		Written	Oral	Using Number	Using Graphical Information	Accessing Information	Providing/Creating Information	Critical Thinking	Planning and Organising	Reviewing and Evaluating	Working Co-operatively with Others	Reviewing Co-operative Contribution
H9E2 44	Data Security (SCQF level 4)		S4			S4					S4	
H9J0 44	Digital Forensics (SCQF level 4)		S4			S4		S4	S4	S4		
H9HY 44	Ethical Hacking (SCQF level 4)		S4			S4		S4	S4	S4	S4	
H9E2 45	Data Security (SCQF level 5)					S5						
H9J0 45	Digital Forensics (SCQF level 5)	S5	S5			S5		S5	S5	S5		
H9HY 45	Ethical Hacking (SCQF level 5)	S5	S5	S5	S5	S5		S5	S5	S5		
H9E2 46	Data Security (SCQF level 6)	S6	S6			S6					S6	
H9J0 46	Digital Forensics (SCQF level 6)	S6	S6			S6		S6	S6	S6		
H9HY 46	Ethical Hacking (SCQF level 6)	S6	S6	S6	S6	S6		S6	S6	S6		

5.4 Assessment Strategy for the qualification

In most Units, the Evidence Requirements take a holistic approach to the generation of evidence to show competence by requiring two items of evidence. These are:

1 evidence of cognitive competence (knowledge and understanding).
2 evidence of practical competence (practical abilities).

The Support Notes provide guidance on the instruments of assessment that could be used to generate the evidence (in the section entitled 'Guidance on Approaches to Assessment').

The following table summarises this **guidance** (and is not mandatory). Alternative forms of assessment are acceptable so long as they satisfy the Evidence Requirements for each Unit. In most cases, the suggested approach to assessment combines all of the knowledge into one assessment and all of the practical skills into one assessment.

Unit		Assessment		
		Outcome 1	**Outcome 2**	**Outcome 3**
H9E2 44	Data Security (SCQF level 4)	Test		Checklist
H9J0 44	Digital Forensics (SCQF level 4)	Test		Activity log
H9HY 44	Ethical Hacking (SCQF level 4)	Test		Checklist
H9E2 45	Data Security (SCQF level 5)	Case study	Test/Report	Report/Presentation
H9J0 45	Digital Forensics (SCQF level 5)	Test	Practical assignment	
H9HY 45	Ethical Hacking (SCQF level 5)	Test		Case study
H9E2 46	Data Security (SCQF level 6)	Essay	Case study	Simulation
H9J0 46	Digital Forensics (SCQF level 6)	Test	Practical exercise/Case study and Report	
H9HY 46	Ethical Hacking (SCQF level 6)	Test	Test	Checklist and Report

Most Units provide alternative approaches to assessment to those summarised above. For example, several Units suggest the use of a web log to record candidate activity over the life of the Unit, which would generate the required evidence.

There may be opportunities to integrate assessment between Units.

6 Guidance on approaches to delivery and assessment

A practical hands-on approach to learning should be adopted to engage learners and exemplify key concepts. However, all practical activities should be underpinned with appropriate knowledge before learners commence these activities.

It is recommended that, as learners progress through the Units at SCQF levels 4, 5 and 6, they are encouraged to increasingly develop responsibility for their own learning and are given opportunities to gain practical experience wherever possible.

Where there are institutional based restrictions on access to resources such, learners should be encouraged to gain experience of their use out with their formal learning environment while, at all times, adhering to appropriate safety, legal and etiquette guidelines.

When progressing through the Data Security Units learners should use the knowledge and tools that are available to defend personal and corporate data from cyber-attacks in the case studies. Learners should be given the chance to create a solution that could prevent data security breaches and take into account legal and ethical considerations.

When progressing through the Digital Forensics Units learners will be introduced to the principles and integrity of digital forensic process. The Units are intended for learners to use legal, professional and ethical application of digital forensics and give a comprehensive understanding of data acquisition, data analysis and the reporting of forensic examination through a practical hands-on approach.

When progressing through the Ethical Hacking Units learners should distinguish between the basic methods used by malicious and ethical hackers to compromise computer systems, as well as applying these in a controlled environment. The learners should be reminded at all times to adhere to the law and not to use any skills acquired without agreement.

In general, teaching should be exemplified in terms of features of cyber security that are appropriate for the learners, that they can relate to and recognise the benefits in their use.

6.1 Sequencing/integration of Units

The recommended sequence of delivery of the Units is:

Data Security → Ethical Hacking → Digital Forensics

The Data Security Units provide a relatively gentle introduction into the field of cyber security, after which learners can undertake the more specialised Units (*Ethical Hacking* and *Digital Forensics*). In fact, either *Ethical Hacking* **or** *Digital Forensics* could be attempted after *Data Security*. However, the insights gained by undertaking *Ethical Hacking* may assist learners in their forensic work.

It is possible for evidence to be gathered simultaneously to meet more than one performance criterion. For example, if a learner applies basic practical methods of protecting personal data to meet a performance criterion in the *Data Security* Unit then, provided it has been recorded accurately and meets the demand of a specific performance criterion, this can be used as part of the evidence for the relevant *Ethical Hacking* Unit.

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
- If candidates have prior knowledge it would be acceptable to sit assessment without teaching taking place.

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

The NPAs in Cyber Security at SCQF levels 4, 5 and 6 are a new qualification. There are, therefore, no direct matches with Units of previous qualifications. However, if, in the course of progressing through another award (eg *Cyber Security Fundamentals* Unit at SCQF level 4), a learner has produced evidence which matches the Performance Criteria in the NPAs Cyber Security, then that evidence is acceptable and may be added to the learner's portfolio.

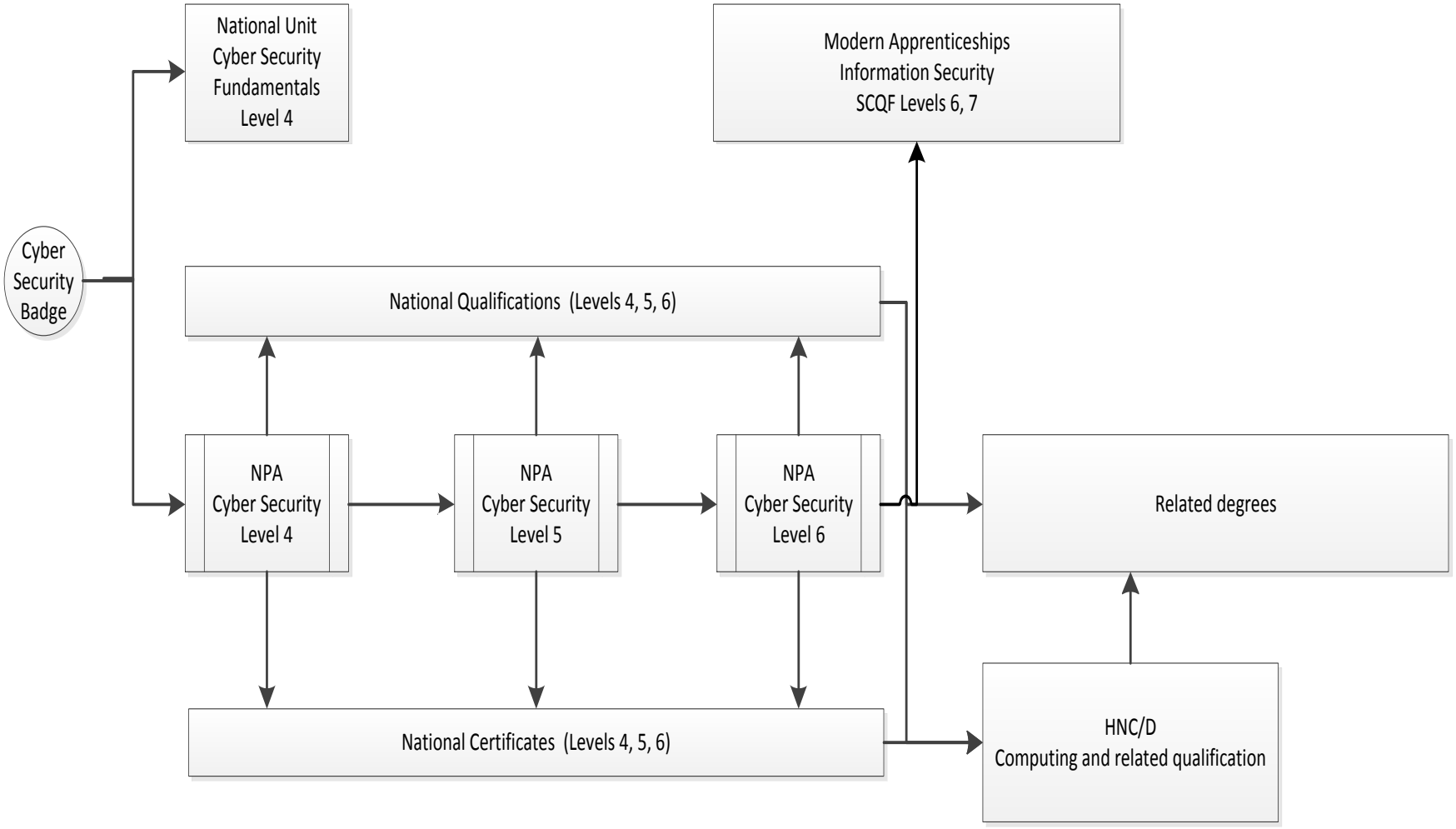
The following sub-sections outline how existing SQA Unit(s) may contribute to this Group Award. Additionally, they also outline how this Group Award may be recognised for professional and articulation purposes.

6.2.1 Articulation and/or progression

The NPAs in Cyber Security have clear hierarchical structures composed of three National Units at each of the levels: SCQF level 4, SCQF level 5 and SCQF level 6. This provides a clear pathway for learners to progress through the levels.

In addition to progression within the hierarchy, learners may progress to external qualifications. Suitable awards for progression include: National Courses, National Certificates, Higher National Certificates and degree courses.

The following diagrams show some of the routes. It is not exhaustive but merely illustrative of the types of routes that learners could pursue.


National Unit
Cyber Security
Fundamentals
Level 4
Modern Apprenticeships
Information Security
SCQF Levels 6, 7
Cyber
Security
Badge
National Qualifications (Levels 4, 5, 6)
NPA
Cyber Security
Level 4
NPA
Cyber Security
Level 5
NPA
Cyber Security
Level 6
Related degrees
National Certificates (Levels 4, 5, 6)
HNC/D
Computing and related qualification

The most relevant National Certificate (NC) programme to progress to is NC Computing with Digital Media. The NPAs are embedded within that award so articulating learners will have at least three credits towards the NC qualification (see Section 6.2.3).

The most relevant Higher National Certificate (HNC) programme to progress to is HNC Computing. It should be noted that possession of any one of these NPAs (alone) is not sufficient for direct articulation to the HNC. Learners would have to progress to the corresponding NC award before progressing to the HNC.

6.2.2 Professional recognition

There is no professional recognition for these awards. However, special interest groups and employers were consulted throughout the development of these awards. It is hoped that professional recognition will be received at a later date, once the awards are embedded as part of the cyber security education portfolio.

6.2.3 Credit transfer

The NPAs in Cyber Security are a new qualification composed of entirely new Units. There is therefore no credit transfer from other Units applicable.

The component Units (at each level) are embedded in the corresponding NC Computing with Digital Media qualification. For example, the three Units in the NPA at level 4 are included in the NC Computing with Digital Media qualification at the same level and, therefore, contribute three credits towards that award.

6.3 Opportunities for e-assessment

The knowledge and understanding of all the Units can be assessed through the SOLAR— **www.sqasolar.org.uk.** If your centre is not already on SOLAR you can complete the form on the SOLAR website and get immediate access. The SOLAR website contains training materials and answers many of the common questions you may have. If you would like to know more contact the SOLAR team on **solar@sqa.org.uk**.

If evidence is produced by means of an e-portfolio, learners are required to collate a portfolio of evidence which may take a variety of digital forms, eg text, graphics, webpages, video clips, audio clips. This may be stored in an appropriate online platform.

6.4 Support materials

Assessment Support Packs will be produced and available to view on SQA's secure site, one for each of the nine Units in the awards. The support packs will provide detailed assessment guidelines and advice as well as exemplars of valid evidence.

6.5 Resource requirements

Centres will require access to a range of hardware and software to facilitate the delivery of these awards, in addition to having teaching staff with the requisite knowledge and experience to deliver the component Units.

The qualification has been designed to be delivered in any (approved) school or college with existing Computing human and computing resources. No special approval requirements are necessary for such centres. While CPD is desirable, and may be essential for some teachers and lecturers, the contents of the awards should be deliverable by any teacher of Computing Science in an approved Scottish school or college.

Some specific technical resources will be required by centres relating to hardware and software for digital forensics and hacking. A particular consideration will be the existing security arrangements (such as firewalls) that are in place in many centres may conflict with the needs of the component Units. One potential resolution to the hardware requirements and security restrictions is the use of simulation, which is discussed in each appropriate Unit (see the Support Notes).

The Ethical Hacking Units pose specific issues. In order to deliver these, centres will need to provide access to a range of appropriate current Open Source Intelligences on the internet. Additionally a sandboxed environment will need to be provided for practical activities. This could be by bare metal hardware via an isolated network or VLAN, or via virtualisation options. It is strongly recommended that learners sign an additional Acceptable Use Policy defining the scope of resources and activities appropriate to their studies as part of the ethical hacking Unit(s).

7 General information for centres

Equality and inclusion

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

Internal and external verification

All instruments of assessment used within this/these qualification(s) should be internally verified, using the appropriate policy within the centre and the guidelines set by SQA.

External verification will be carried out by SQA to ensure that internal assessment is within the national guidelines for these qualifications.

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

8 Glossary of terms

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

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

- 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. (**Note to writer:** delete if not applicable to product type)

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 Higher National Unit credit (irrespective of level) is equivalent to 8 SCQF credit points.

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

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

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

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 candidates for the Unit which has been revised where they are expected to complete the Unit before its finish date.

Version Number	Description	Date

Acknowledgement

SQA acknowledges the valuable contribution that Scotland's schools, colleges, universities and industry representatives have made to the development of this qualification.

9 General information for learners

This section will help you decide whether this is the qualification for you by explaining what the qualification is about, what you will need to do during the qualification and opportunities for further learning and employment.

This qualification is about making the online environment safe; both for you, as an individual, and the wider community. Cyber security is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.

The qualification has three parts: **(1) Data Security**; **(2) Digital Forensics**; and **(3) Ethical Hacking.**

Data Security

The specific aim of the Data Security Units is to place data security within the context of the real world and explore current practice in corporate data security. This includes the legal and ethical considerations, and the practical methods to protect personal and corporate data. The Units will introduce you to the concepts around personal and corporate data security, including aspects of legal and ethical obligations.

Digital Forensics

The Digital Forensics Units are designed to develop your knowledge and skills in digital forensics examination. You will gain knowledge of the principles and the integrity of the process involved in forensically examining digital evidence. You will gain practical skills in identifying evidential sources across a range of digital devices and mediums. Using these sources of evidence, you will then analyse and interpret data, its relevancy to an enquiry under investigation and the subsequent reporting of that information.

Ethical Hacking

The purpose of the Ethical Hacking Units is to develop a competent understanding of tools and techniques used by malicious and ethical hackers. You will gain an understanding of the potential threats and tools that can be used by malicious hackers to target individuals and organisations. By the end of this Unit you will have the ability to implement techniques and technologies used to defend systems from attack and evaluate the Scottish, UK and EU legislation and ethics of hacking.

The assessment will be straight-forward. It will not take up a great deal of time. Both your knowledge and practical abilities will be assessed. Your teacher will decide what types of assessment to use, which could involve multiple choice tests or oral questions or maintaining a log book. Your practical abilities may be assessed through practical tasks or case studies.

On completion of each award you may progress to one of a number of further qualifications in this, or a related, area. This qualification is available at three levels and you may progress to the next level if you wish to continue your studies. There are also opportunities to progress to Higher National or degree courses if you have the appropriate set of qualifications. If you possess other qualifications and have previous work experience in computing, this award may also lead to employment in a computer security role. The number, and nature, of job roles in this field are growing fast and it is hoped that this award will be your springboard to a career in computer security.