Group Award Specification for:

PDA Cyber Resilience (SCQF level 7)

Group Award Code: GR3R 47

PDA Cyber Resilience (SCQF level 8)

Group Award Code: GR3T 48

PDA Cyber Resilience (SCQF level 9)

Group Award Code: GR3V 49

Validation date: May 2020

Date of original publication: July 2020

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 qualifications
- provide a guide for new staff involved in offering the qualifications
- inform course managers, teaching staff, assessors, learners, employers and higher education institutes (HEIs) of the aims and purpose of the qualifications
- provide details of the range of learners the qualifications are suitable for and progression opportunities

Background

These qualifications are part of a suite of awards in Cyber Security/Resilience, spanning SCQF levels 4 to 9, which were developed in response to a national (and international) focus on cyber 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[1]. The development of these qualifications was part-funded by the Scottish Government.

These qualifications provide a complementary route to learning aimed at people who are at non-cyber security professional roles in the existing workforce with a desire to develop awareness and knowledge of cyber resilience practices. The suite of cyber security/resilience awards is illustrated in Figure 1.

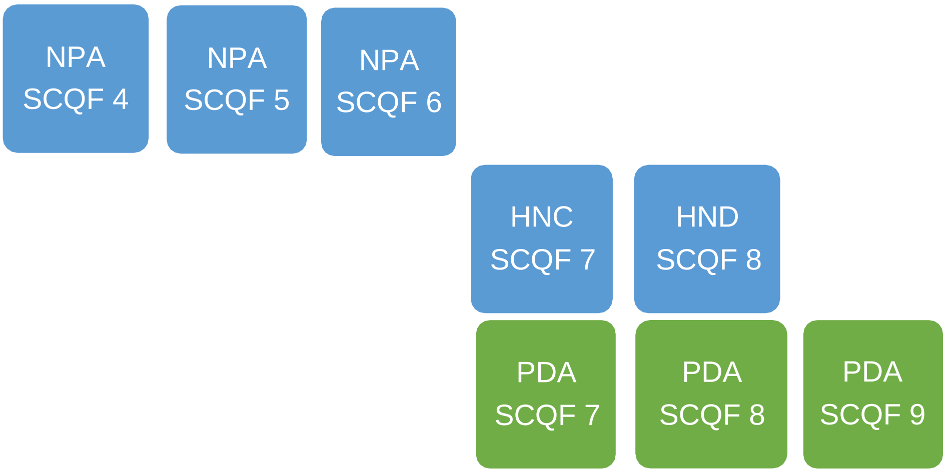


Figure 1: Qualifications and levels

Rationale

The title of the qualifications (Cyber Resilience) is used to represent coverage of the core cyber security awareness themes for the wider workforce (threats and vulnerabilities, cyber security controls and intrusion detection and response).

The qualifications are intended for learners who typically work in a wide range of roles not directly related to cyber security, but where cyber resilience is becoming an increasingly important factor to their roles.

[1] https://www.gov.scot/Publications/2017/11/6231

A number of entry and exit points exist and also full progression through the qualification levels. Figure 2 illustrates the most common entry and exit points.

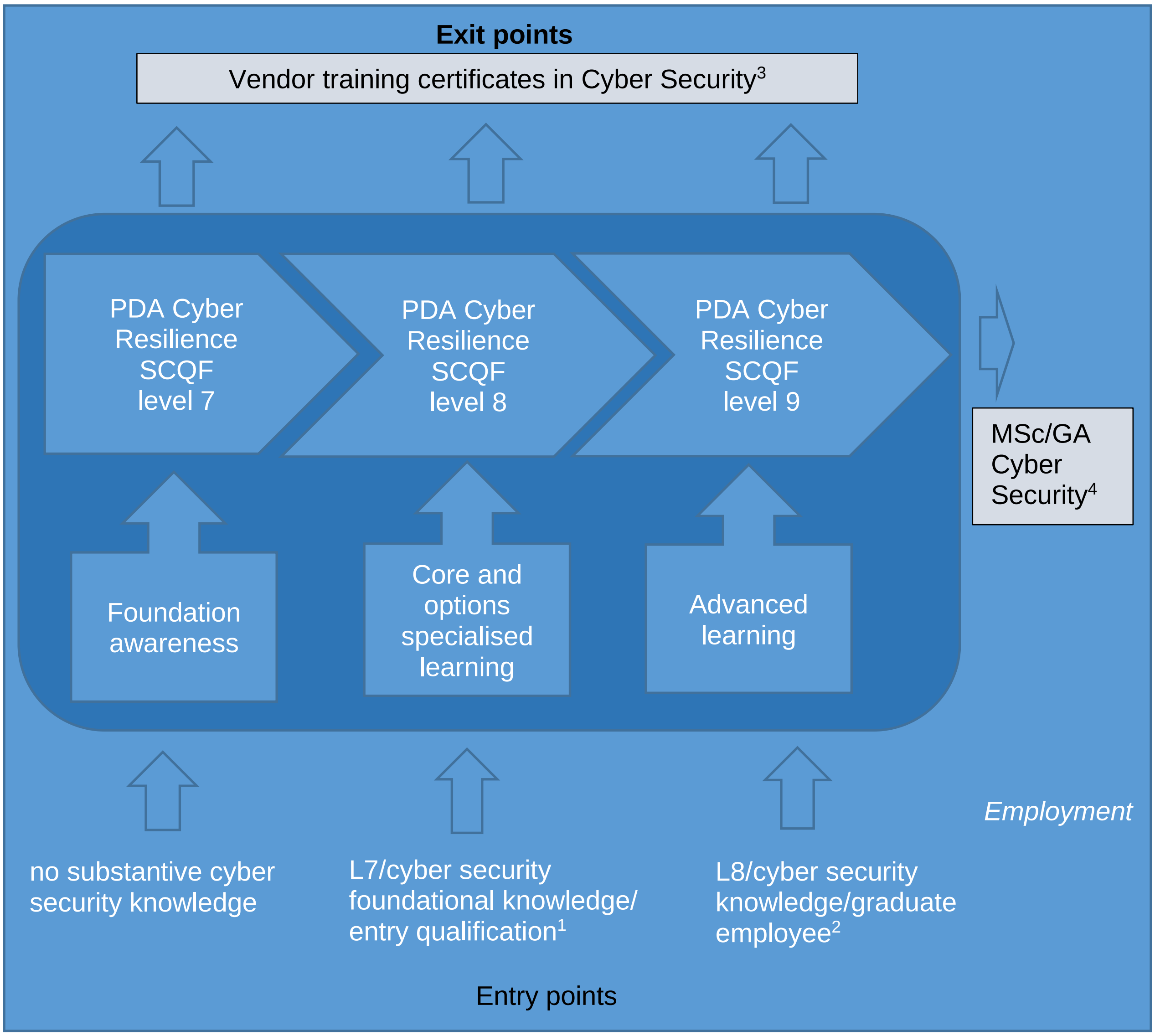

Exit points
Vendor training certificates in Cyber Security[3]
PDA Cyber Resilience SCQF level 7
PDA Cyber Resilience SCQF level 8
PDA Cyber Resilience SCQF level 9
MSc/GA Cyber Security[4]
Foundation awareness
Core and options specialised learning
Advanced learning
Employment
no substantive cyber security knowledge
L7/cyber security foundational knowledge/ entry qualification[1]
L8/cyber security knowledge/graduate employee[2]
Entry points

Figure 2: Entry and exit points

Entry points

The qualifications aim to attract four types of learner who are expected to enter through one of the following routes:

1 Direct entry from employment. Learners will typically seek to develop their awareness and understanding of cyber resilience in the context of their own employment.

2 Direct entry from employment. Learners will typically seek to develop their awareness and understanding in order to support a career change into a more cyber security focused role with their own or another employer.

3 Direct entry from unemployment. Learners will typically seek to develop their awareness and understanding in order to pursue a career in a cyber security related role with an employer.

4 Direct entry from university. Learners will typically be new graduate hires who may lack a foundational understanding of applied cyber security.

Entry qualifications

There are no formal entry qualification requirements for any level:

- Entry to level 7 has no pre-requisites and is the recommended entry point for most learners.
- Entry to level 8 may be from level 7 or direct entry may benefit from completion of relevant foundation vendor qualifications in Cyber Security, including Cyber Essentials, CompTIA Security + etc.
- Graduates commencing employment with a technical degree and some cyber security knowledge could enter level 9 directly.

The qualification at SCQF level 7 will be suitable for leaners with no previous background in cyber security, who are seeking to develop a robust foundational awareness. The qualification at SCQF level 8 will be suitable for learners with some previous knowledge of cyber security or those progressing from the level 7 PDA in Cyber Resilience. The qualification at SCQF level 9 will be suitable for learners with a graduate-level qualification in a STEM area who wish to develop cyber security specialisations.

Section 4 (Recommended entry) provides further information about the types of qualifications and experiences expected from learners who wish to undertake this award.

Progression

Learners may progress to further cyber security specific learning and training, education or employment. The qualifications should permit learners to progress to a range of pathways in cyber security (or related subjects). Learners completing the SCQF level 9 could consider specialising in cyber security related employment as entry-level cyber security analysts. Those completing lower levels are likely to require further training before being ready to enter cyber security related employment.

Progression options include that:

- There are a wide range of vendor training and certifications that learners could progress onto, including Cyber Essentials, CompTIA Security + etc.
- Learners could progress to the HNC and HND in Cyber Security after having completed the level 7/8 units in the PDAs.
- Exiting from the level 9 PDA would enable learners to consider progressing to the Graduate Apprenticeship in Cyber Security at SCQF levels 10 and 11 or certain conversion MSc in Cyber Security. These options would be subject to individual entry requirements of individual universities.

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

- IT support/security analyst
- Systems administrator
- Network engineer
- Penetration tester
- Cyber analyst/operations analyst

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

2 Qualifications structure

The group awards are available at **three levels**: SCQF levels 7, 8 and 9.

2.1 Structure

PDA Cyber Resilience at SCQF level 7

This group award is made up of four mandatory units with 4 SQA credits. Learners must achieve all the mandatory units.

4 code	2 code	Unit title	SQA credit	SCQF credit points	SCQF level
HT9V	34	Cyber Resilience	1	8	7
J0H9	34	Data Security	1	8	7
J0HH	34	Professionalism and Ethics in Cyber Security	1	8	7
J0HF	34	Social Engineering	1	8	7

PDA Cyber Resilience at SCQF level 8

This group award is made up of 4 SQA credits.

Mandatory units

Learners must achieve all the mandatory units.

4 code	2 code	Unit title	SQA credit	SCQF credit points	SCQF level
J4BA	35	Threat Analysis	1	8	8
J4BB	35	Cyber Security Controls	1	8	8
J4BC	35	Intrusion Detection, Analysis and Response	1	8	8

Optional units

Learners must achieve at least 1 SQA credit from the following optional units.

4 code	2 code	Unit title	SQA credit	SCQF credit points	SCQF level
H17M	34	Intrusion Prevention Systems	1	8	7
J0HB	34	Penetration Testing	1	8	7
J0HK	34	Ethical Hacking	1	8	7
J4BF	34	Cryptography: Practical Applications	1	8	7
J4BH	34	Software Security	1	8	7
J4BG	34	Application Security	1	8	7

PDA Cyber Resilience at SCQF level 9

This group award is made up of three mandatory units with 4 SQA credits. Learners must achieve all the mandatory units.

4 code	2 code	Unit title	SQA credit	SCQF credit points	SCQF level
J4BD	36	Cyber Resilience	2	16	9
J27N	35	Network Security Monitoring	1	8	8
J4BE	36	Cyber Security Risk Management	1	8	9

The mandatory units are the main building blocks and reflect the aims and purposes of each award. The optional units in the level 8 PDA provide subject specific learning in specific areas, such as penetration testing, cryptography, software security, and application security.

The choice of optional units means the award can be tailored for different learner cohorts.

Whilst there are no specific vendor awards included in the qualifications, there will be opportunities for individual centres to embed vendor materials as a vehicle to deliver units that closely match several of the popular vendor curricula.

Furthermore, centres may wish to offer the chance for learners to gain vendor qualifications in addition to achieving the units. Examples of this practice may include:

- CompTIA security plus
- Cyber essentials

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

3 Aims of the qualifications

The principal aim of the qualifications is to introduce cyber security to learners already employed across the wider workforce, to encourage interest in this emerging discipline as a potential future career and to improve cyber security knowledge for all learners irrespective of their vocational goals.

The qualifications aim to provide **foundation knowledge and skills** in cyber security to increase awareness and develop deeper knowledge and appropriate skills of the discipline among learners. The qualifications will also raise awareness of the societal aspects of cyber security.

The aims of the qualifications are categorised as general aims and specific aims. General aims relate to broad educational objectives; specific aims relate to the vocational area. Please note that the general aims may be repeated in the specific aims but contextualised in the subject area. Although the qualifications exist at three levels (SCQF levels 7, 8 and 9), they should be considered a single **suite** of awards, sharing the same aims from level to level.

The aims have been ordered to reflect their broad, relative importance (within each category).

3.1 General aims of the qualification

1 To contribute to strengthening the cyber security and resilience of Scottish organisations through raising awareness and specialist competencies.
2 To develop cyber security and resilience skills and knowledge consistent with the SCQF levels of the qualifications.
3 To develop broad vocational competencies in cyber security and resilience relevant to employment across sectors.
4 To stimulate interest in cyber security and resilience.

3.2 Specific aims of the qualification

5 To focus on developing cyber security and resilience knowledge and skills in an employment context.
6 To develop an understanding of the nature of information privacy, confidentiality and availability within organisations.
7 To develop an awareness of contemporary cyber security threats to an organisation’s information and information systems.
8 To develop an awareness of the range of typical security controls that organisations implement to protect information and how these need to be reviewed and revised to respond to changing threat actor activities.
9 To develop an understanding of how organisations identify and manage vulnerabilities in their information systems and risk to information.
10 To appreciate intrusion detection and how the monitoring and detection of intrusions is typically managed.
11 To recognise and respond to cyber security incidents and enable recovery.
12 To appreciate the legal and regulatory environment for cyber security and how compliance is achieved.

The general aims apply to all levels. The following guidance relates to aims specific to levels.

The qualification at **SCQF level 7** aims to provide a basic, introductory qualification in the core principles and practices of cyber resilience. It is suitable for all learners who wish to develop their **cyber security awareness** in support of their contribution to strengthening the cyber resilience of their employer organisation. At this level, developing vocational competencies and Core Skills, improving cyber security awareness, and appreciating cyber security in an organisational context are particularly significant.

The qualification at **SCQF level 8** will deepen knowledge and skills through the application of a range of related cyber security processes. It offers progression from the qualification at SCQF level 7, by providing a broader introduction to cyber security and offering specialisations relevant to a wide range of sectors.

The qualification at **SCQF level 9** reinforces the core principles at a higher level and introduces advanced cyber security process topics, including Network Security Monitoring and Cyber Security Risk Management. As well as providing progression from the SCQF level 8 qualification, it is also suitable for learners who may have studied a technical qualification in computing/engineering/data analysis, who have recently entered the workforce and seek to develop their interest in cyber security as a potential career specialisation.

These qualifications provide a solid foundation and raise awareness of cyber security operations. Progression from the PDAs as general cyber security awareness qualifications can support future progression to cyber security pathways for those interested in developing cyber security careers.

4 Recommended entry to the qualifications

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

No previous experience of cyber security is required (at any level). However, direct entry to higher levels (particularly SCQF level 9) will require appropriate computational and numeracy skills. The qualifications at SCQF levels 7 and level 8 may be entered directly without previous experience of the subject area; it is recommended that learners undertake the award at SCQF level 7 before attempting SCQF level 8. Direct entry to SCQF level 9 is possible for suitably qualified learners.

It is desirable for learners to possess awareness of information systems and basic computer networks before attempting this award (at any level). This may be evidenced by possession of **one or more** of the following qualifications:

- Core Skills in *Information and Communication Technology (ICT)* and *Numeracy* at an appropriate level
- National Units in Computing or Mathematics or a related subject area
- National Progression Award (NPA) in a range of subjects at SCQF level 4, 5 or 6
- National 4/5 in Computing Science
- National 4/5 in Mathematics

Given the multi-disciplinary nature of cyber security, a wide range of subjects may provide the necessary foundation for attempting these awards.

These qualifications are particularly suitable for a wide range of adult learners in employment who wish to acquire cyber security knowledge and skills, or learners who wish to commence to retrain in this field by first developing some foundational awareness. The entry requirements for these learners will vary from learner to learner, depending on their individual experiences and motivations.

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 the qualification. The information would be used to identify if additional learning support needs to be put in place for learners whose Core Skills profile is below the recommended entry level or whether learners should be encouraged to do an alternative level or learning programme.

Core Skill	Recommended SCQF entry profile	Associated assessment activities
Communication	5	Report and evaluation writing
Numeracy	5	Basic mathematical operation and understanding
Information and Communication Technology (ICT)	5	Research and present information
Problem Solving	5	Analysis
Working with Others	5	Participating in collaborative sessions, exploring aspects in own work environment

5 Additional benefits of the qualification in meeting employer needs

These qualifications are 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 qualifications. 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 doing these qualifications.

5.1 Mapping of qualification aims to units

Code	**Unit title**	**Aims**											
		1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
PDA Cyber Resilience SCQF level 7													
HT9V 34	Cyber Resilience	X	X	X	X	X	X	X	X	X	X	X	
J0H9 34	Data Security	X	X	X	X	X	X						
J0HH 34	Professionalism and Ethics in Cyber Security	X	X	X	X	X							X
J0HF 34	Social Engineering	X	X	X	X	X	X	X					
PDA Cyber Resilience SCQF level 8													
Mandatory units													
J4BA 35	Threat Analysis	X	X	X	X	X	X	X		X			
J4BB 35	Cyber Security Controls	X	X	X	X	X	X		X				
J4BC 35	Intrusion Detection, Analysis and Response	X	X	X	X	X	X				X	X	
Optional units													
H17M 34	Intrusion Prevention Systems	X	X	X	X	X	X			X			
J0HB 34	Penetration Testing	X	X	X	X	X	X						
J0HK 34	Ethical Hacking	X	X	X	X	X	X						
J4BF 34	Cryptography: Practical Applications	X	X	X	X	X	X						
J4BH 34	Software Security	X	X	X	X	X	X						
J4BG 34	Application Security	X	X	X	X	X	X						
PDA Cyber Security SCQF level 9													
J4BD 36	Cyber Resilience	X	X	X	X	X	X	X	X	X	X	X	X
J27N 35	Network Security Monitoring	X	X	X	X	X	X						
J4BE 36	Cyber Security Risk Management	X	X	X	X	X	X						

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

The Cyber Security Resilience National Occupational Standards are organised in three sub-disciplines (March 2020):

1 Identify cyber security threats and vulnerabilities.
2 Protect against cyber security threats.
3 Respond to and recover from cyber security attack.

Code	**Unit title**	**National Occupational Standard**		
		Identify cyber security threats and vulnerabilities	Protect against cyber security threats	Respond to and recover from cyber security attack
		TECIS600201	**TECIS600202**	**TECIS600203**
HT9V 34	Cyber Resilience	X		
J0H9 34	Data Security	X	X	
J0HH 34	Professionalism and Ethics in Cyber Security	X	X	X
J0HF 34	Social Engineering	X	X	
J4BA 35	Threat Analysis	X		
J4BB 35	Cyber Security Controls		X	
J4BC 35	Intrusion Detection, Analysis and Response			X
H17M 34	Intrusion Prevention Systems		X	
J0HB 34	Penetration Testing	X		
J0HK 34	Ethical Hacking	X		
J4BF 34	Cryptography: Practical Applications		X	
J4BH 34	Software Security		X	
J4BG 34	Application Security		X	
J4BD 36	Cyber Resilience	X		
J27N 35	Network Security Monitoring	X		
J4BE 36	Cyber Security Risk Management	X	X	X

5.3 Mapping of Core Skills development opportunities across the qualifications

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

Unit code	Unit title	Communication			Numeracy		ICT		Problem Solving			Working with Others	
		Written (Reading)	Written (Writing)	Oral	Using Number	Using Graphical Information	Accessing Information	Providing/Creating Information	Critical Thinking	Planning and Organising	Reviewing and Evaluating	Working Co-operatively with Others	Reviewing Co-operative Contribution
HT9V 34	Cyber Resilience								E(5)	E(5)	E(5)		
J0H9 34	Data Security	S(5)	S(5)						S(5)	S(5)	S(5)	S(5)	
J0HH 34	Professionalism and Ethics in Cyber Security	S(6)	S(6)										
J0HF 34	Social Engineering	S(5)	S(5)						E(5)	S(5)	S(5)	S(5)	
J4BA 35	Threat Analysis	S(5)	S(5)				S(5)	S(5)	E(6)	S(5)	S(5)		
J4BB 35	Cyber Security Controls	S(5)	S(5)				S(5)	S(5)	E(6)				
J4BC 35	Intrusion Detection, Analysis and Response	S(5)	S(5)				S(5)	S(5)	E(6)	S(5)	S(5)		
J0HB 34	Penetration Testing								E(5)	E(5)	E(5)		
J0HK 34	Ethical Hacking						E(5)		E(6)	E(6)	E(6)		
J4BF 34	Cryptography: Practical Applications	S(5)	S(5)				S(5)	S(5)	E(6)	S(5)	S(5)		
J4BH 34	Software Security	S(5)	S(5)				S(5)	S(5)	E(6)	S(5)	S(5)		
J4BG 34	Application Security	S(5)	S(5)				S(5)	S(5)	E(6)	S(5)	S(5)		
J4BD 36	Cyber Resilience	S(6)	S(6)				S(6)	S(6)	S(6)	S(6)	S(6)		
J27N 35	Network Security Monitoring	S(6)	S(6)				E(5)	S(6)	E(6)	S(6)	S(6)		
J4BE 36	Cyber Security Risk Management	S(6)	S(6)						S(6)	S(6)	S(6)		

* The table will be updated if any embedded Core Skills in the new units are identified.

5.4 Assessment strategy for the qualifications

The award may be assessed unit by unit. Assessment support packs or SOLAR assessments are available for all of the mandatory units and some of the optional units. The following table summarises the types of evidence required for each of the units. Please check the unit specification for each unit for more information about assessment requirements.

Unit code	Unit title	Assessment				
		Outcome 1	**Outcome 2**	**Outcome 3**	**Outcome 4**	**Outcome 5**
HT9V 34	Cyber Resilience (SCQF level 7)	Knowledge evidence, product evidence and performance evidence for all three outcomes			Not applicable	Not applicable
J0H9 34	Data Security	Knowledge evidence			Not applicable	Not applicable
		Not applicable	Product evidence			Not applicable
J0HH 34	Professionalism and Ethics in Cyber Security	Knowledge evidence			Not applicable	Not applicable
J0HF 34	Social Engineering	Knowledge evidence			Not applicable	Not applicable
		Not applicable		Product evidence	Not applicable	Not applicable
J4BA 35	Threat Analysis	Knowledge evidence	Product evidence	Knowledge evidence	Knowledge evidence	Product evidence
J4BB 35	Cyber Security Controls	Knowledge evidence		Product evidence	Not applicable	Not applicable
J4BC 35	Intrusion Detection, Analysis and Response	Knowledge evidence			Not applicable	Not applicable
H17M 34	Intrusion Prevention Systems	Knowledge evidence	Product evidence	Not applicable	Not applicable	Not applicable
J0HB 34	Penetration Testing	Product evidence				Not applicable
J0HK 34	Ethical Hacking	Knowledge evidence				Not applicable
		Not applicable	Product evidence/performance evidence			Not applicable

<table>
<tr><th rowspan="2">Unit code</th><th rowspan="2">Unit title</th><th colspan="5">Assessment</th></tr>
<tr><th>Outcome 1</th><th>Outcome 2</th><th>Outcome 3</th><th>Outcome 4</th><th>Outcome 5</th></tr>
<tr><td>J4BF 34</td><td>Cryptography: Practical Applications</td><td colspan="2">Knowledge evidence</td><td>Product evidence</td><td>Not applicable</td><td>Not applicable</td></tr>
<tr><td>J4BH 34</td><td>Software Security</td><td>Knowledge evidence</td><td colspan="2">Product evidence</td><td>Not applicable</td><td>Not applicable</td></tr>
<tr><td>J4BG 34</td><td>Application Security</td><td colspan="2">Knowledge evidence</td><td>Product evidence</td><td>Not applicable</td><td>Not applicable</td></tr>
<tr><td>J4BD 36</td><td>Cyber Resilience (SCQF level 9)</td><td colspan="5">Product evidence</td></tr>
<tr><td rowspan="2">J27N 35</td><td rowspan="2">Network Security Monitoring</td><td colspan="4">Knowledge evidence</td><td rowspan="2">Not applicable</td></tr>
<tr><td colspan="2">Not applicable</td><td colspan="2">Product evidence</td></tr>
<tr><td>J4BE 36</td><td>Cyber Security Risk Management</td><td colspan="3">Knowledge evidence</td><td>Product evidence</td><td>Not applicable</td></tr>
</table>

6 Guidance on approaches to delivery and assessment

These qualifications aim to deliver a broad, but relatively shallow, range of knowledge and skills in cyber security. The PDA in Cyber Resilience at SCQF level 7 represents a foundational introduction to the subject area, which should be achievable by most learners, irrespective of their previous knowledge and skills. At SCQF level 8 the award presents a more challenging curriculum and is ideally a progression from SCQF level 7 for most learners.

The PDAs in Cyber Resilience are designed for learners in employment in the wider workforce who want to develop foundation knowledge and skills in cyber security to increase their awareness and develop deeper knowledge and appropriate skills of the discipline. Learners may seek to undertake one of the industry standard vendor certification programmes in broad cyber security and/or to progress to more specialist areas of cyber security. It is recommended that a practical approach to learning is adopted, whereby learners are given the opportunity to apply their knowledge to problems using appropriate investigative and research-based approaches.

The group awards have been designed so that learners get a taste of the main areas in cyber security. The flexibility of the optional units at SCQF level 8 will allow centres to tailor the qualification at this level built around the key concepts of cyber security but allowing them full utilisation of their staff's skills sets.

The qualifications can be delivered in several ways, including full-time, part-time or day release. Part-time delivery may be the best approach for mixed cohorts of learners from different employers. Learners may be either self-motivated or sponsored by their employer. There is a strong case for offering the SCQF level 7 foundational programme as full-time fast-track, particularly if employers seek to place a full cohort of learners, though day-release should also be considered.

Centres could adopt the following suggested delivery methods:

- Lectures
- Tutorials
- Virtual learning environments
- Projects
- Group work
- Case studies

A distinguishing feature of cyber security is the need to protect data of different types, to understand the threat landscape, vulnerabilities in information systems, the controls that can be used to mitigate these and how to identify and deal with cyber security breaches. It is recommended that teaching and learning involves building foundational principles that learners can then develop and explore, including within their own workplace where practical to do so.

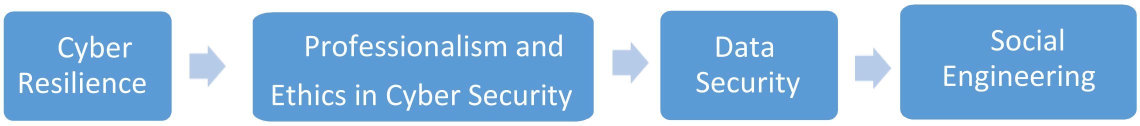
It is also recommended that learners should explore real world case studies, including up to date sources of threat intelligence and that they are exposed to real scenarios whenever possible.

A wide range of online resources exist to aid teaching and learning, ranging from YouTube (**http://www.youtube.com**) for instructional videos on cyber security to resources such as Cyber Essentials **(https://www.cyberessentials.ncsc.gov.uk/).**

6.1 Sequencing/integration of units

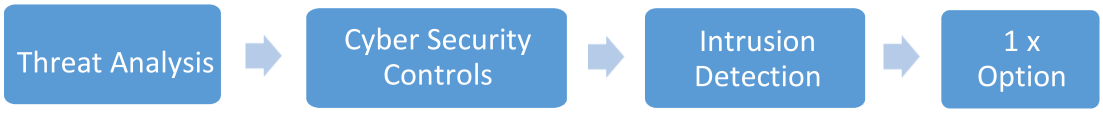
The sequence of delivery is at the discretion of each centre, but the following recommendations may help with planning for delivery:

Level 7



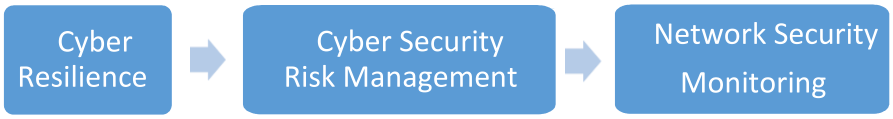
The *Cyber Resilience* unit should be delivered and assessed prior to the commencement of the other units. The *Professionalism and Ethics in Cyber Security* unit should be delivered before the *Data Security* unit to ensure that learners are exposed to the importance of data legislation. At this level a completely integrated approach to delivery could be adopted where the four units could be delivered as a single combined curriculum, over 160 hours, with no specific unit boundaries.

Level 8



The three mandatory units should be delivered and assessed prior to the commencement of the optional unit. The *Threat Analysis* unit should be delivered and assessed prior to the commencement of the other units. The order of the remaining units is less important.

Level 9



The *Cyber Resilience* unit should be delivered and assessed prior to the commencement of the *Cyber Security Risk Management and Network Security Monitoring* units*.*

It is also possible for all units to be delivered separately, where different lecturers are timetabled for different units.

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.

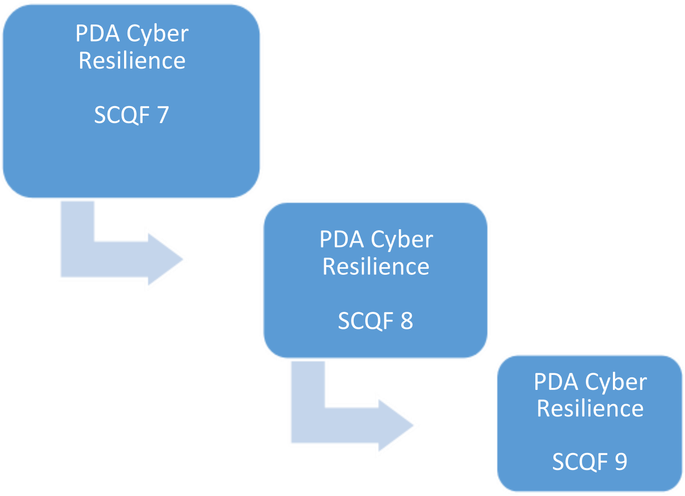
More information and guidance on the *Recognition of Prior Learning* (RPL) may be found on our website **www.sqa.org.uk**.

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

6.2.1 Articulation and/or progression

There are no formal articulation routes for this award. However, the qualifications could lead to potential destinations including Modern or Graduate Apprenticeships and degree/MSc courses in Cyber Security or related disciplines and qualifications at SCQF level 9.

The main progression for this award is from level to level. For example, progressing from SCQF level 7 to SCQF level 9 as illustrated below. In addition, learners could subsequently undertake one of the Industry Standard Cyber Security training certificates such as Cyber Essentials and CompTIA Security +.



6.2.2 Professional recognition

There is no professional recognition for this award. However, learners would be able to undertake the Industry Standard Cyber Essentials and CompTIA Security + or similar.

6.3 Assessment

Opportunities for e-assessment will be presented where knowledge assessment methods such as multiple choice is the chosen method of knowledge 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.

The following assessments are available or currently under development.

Unit title	**E-assessment**	**Assessment Support Pack**
Cyber Resilience (SCQF level 7)	√	√
Data Security	x	√
Professionalism and Ethics in Cyber Security	x	√
Social Engineering	√	x
Threat Analysis	√	x
Cyber Security Controls	√	x
Intrusion Detection, Analysis and Response	√	x
Penetration Testing	x	√
Ethical Hacking	√	√
Cyber Resilience (SCQF level 9)	√	x
Network Security Monitoring	√	x
Cyber Security Risk Management	√	x

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**.

6.4 Resource requirements

The PDAs in Cyber Resilience will require a mixture of general and specialist resources including some specialist hardware, software and support materials for some units. The optional units will require more specialised resources due to their specialised nature.

Every centre will have a different infrastructure and support structure so it would be impossible to provide a prescriptive list of what is required. The table below indicates which units would require general resources (standard PCs and internet search facilities) and those requiring specialist resources (network labs, specialised software, etc).

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.

Unit code	Unit title	General/Specialised unit resource requirements
HT9V 34	Cyber Resilience	General
J0H9 34	Data Security	Specialised — spreadsheets and databases
J0HH 34	Professionalism and Ethics in Cyber Security	General
J0HF 34	Social Engineering	General
J4BA 35	Threat Analysis	General
J4BB 35	Cyber Security Controls	Specialised — antivirus/malware
J4BC 35	Intrusion Detection, Analysis and Response	Specialised — Intrusion detection software
H17M 34	Intrusion Prevention Systems	Specialised — Intrusion prevention software (IPS) and testing
J0HB 34	Penetration Testing	Specialised — penetration testing software
J0HK 34	Ethical Hacking	Specialised — penetration testing software
J4BF 34	Cryptography: Practical Applications	Specialised — cryptography and encryption software
J4BH 34	Software Security	Specialised —security test software
J4BG 34	Application Security	Specialised — client server test deployment and application test software
J4BD 36	Cyber Resilience	General
J27N 35	Network Security Monitoring	Specialised — active network and network monitoring tools
J4BE 36	Cyber Security Risk Management	General

Where there is significant demand for specialised units such as penetration testing and ethical hacking then there may be the case to support the creation of an isolated lab that allows only internal network traffic within the room. This would greatly reduce the possibility of external network issues or attacks, whether deliberate or not. However, as these are current units it is likely that centres already delivering these units on other programmes will have made relevant arrangements.

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.

Whilst such overheads and additional tasks may be a burden, their importance should be stressed 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 assessments used within this/these qualification(s) should be internally verified, using the appropriate policy within the centre and the guidelines set by SQA.

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

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

8 Glossary of terms

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

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

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

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

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

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

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

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

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

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

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

History of changes

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

NOTE: Where a unit is revised by another unit:

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

Version Number	Description	Date

Acknowledgement

SQA acknowledges the valuable contribution that Scotland's colleges 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 should know or be able to do before you start, what you will need to do during the qualification and opportunities for further learning and employment.

The Professional Development Award in Cyber Resilience is available at three levels: SCQF level 7, SCQF level 8 and SCQF level 9. The over-arching aim of the qualifications is to introduce learners already employed across the wider workforce to the main principles of cyber security in order to encourage interest in the discipline. Developing greater cyber security awareness across the workforce is an important objective for many employers seeking to strengthen their cyber resilience. It also supports learners who may require the development of specific cyber security knowledge and skills through changes in their job roles, or for those who seek to explore cyber security as a potential future career.

The qualifications are introductory. You are not expected to know anything about cyber security before you commence them. However, at the higher levels (SCQF level 8 and above) you may need to possess numeracy, digital literacy and computing skills.

The qualification at **SCQF level 7** aims to provide a basic, introductory qualification in the core principles and practices of cyber resilience. It would be suitable for you if you wish to develop your **cyber security awareness** in support of your contribution to strengthening the cyber resilience of your organisation.

The qualification at **SCQF level 8** will deepen knowledge and skills through the application of a range of related cyber security processes. It offers progression from the qualification at SCQF level 7, by providing a broader introduction to cyber security and offering specialisations relevant to a wide range of sectors.

The qualification at **SCQF level 9** reinforces the core principles at a higher level and introduces advanced cyber security process topics, including Network Security Monitoring and Cyber Security Risk Management. If you have studied a technical qualification in computing/engineering/data analysis or have recently entered the workforce and seek to develop your interest in cyber security as a potential career specialisation, this would be a suitable qualification for you.

These qualifications provide a solid foundation and raise awareness of cyber security operations. You may progress to further cyber security specific learning and training, education or employment. For example, there are a wide range of vendor training and certifications that you could progress to, including Cyber Essentials, CompTIA Security + etc, or the HNC/HND in Cyber Security. You might consider progressing to the Graduate Apprenticeship in Cyber Security at SCQF levels 10 and 11 or certain conversion MSc in Cyber Security after successfully completing the level 9 PDA. These options would be subject to entry requirements of individual universities.

A range of employment opportunities exist including IT support/security analyst, Systems administrator, Network engineer, Penetration tester and Cyber analyst/operations analyst. You may require a degree and/or relevant experience before applying for some of these positions.

In addition to these specialist skills, you will also develop a range of Core Skills and employment skills, for example *ICT, Communication* and *Problem Solving*.

You may be assessed in a variety of ways including short tests of your knowledge, practical assignments and project work.