Skills Development Scotland

Graduate Apprenticeships

Framework document for

Cyber Security at

SCQF level 10

September, 2017

European Union

gov.scot

EUROPE & SCOTLAND
European Social Fund
Investing in a Smart, Sustainable and Inclusive Future

Document control

Version history

Version	Revision(s)	Approved by	Date
1.0	Draft	SDS	18.5.17
2.0	Updates from TEG 1	TEG members	21.7.17
3.0	Updates from TEG 2	TEG members	10.8.17
4.0	Updates from TEG 3	TEG members	20.8.17
Final	Final version	TEG members	01.09.17
5.0	Higher Apprenticeship reference	SDS	01.07.19

Terms and abbreviations

Term	Meaning
SDS	Skills Development Scotland
GA(s)	Graduate Apprenticeship(s) / Apprentice(s)
SCQF	Scottish Credit and Qualifications Framework
TEG	Technical Expert Group
QA	Quality Assurance
BSc	Bachelor of Science
IT	Information Technology
UKSPEC	UK Standard for Professional Competence
IEng	Incorporated Engineer
CEng	Chartered Engineer
ICT	Information and Communication Technology
OS	Operating System
HTTP	Hypertext Transfer Protocol
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
IP	Internet Protocol
BGP	Border Gateway Protocol
DNS	Domain Name Server
DBMS	Database Management Software

NIDS	Network Intrusion Detection Systems
HIDS	Host-based Intrusion Detection Systems
IPS	Intrusion Prevention Systems
IDS	Intrusion Detection Systems
OWASP	Open Web Application Security Project
SIEM	Security Information Event Management
SABSA	Sherwood Applied Business Security Architecture
DBSy	Domain Based Security
CVSS	Common Vulnerability Scoring System
STRIDE	Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege
NIST	National Institute of Standards and Technology
Gdpr	General Data Protection Regulation
NCSC	National Cyber Security Centre
PCI-DSS	Payment Card Industry Data Security Standard
FIPS	Federal Information Processing Standard
ISO	International Standards Organisation
IDAM	Identity and Access Management
AV	Anti Virus
GSM	Global System for Mobile Communications
TLS	Transport Layer Security
SSL	Secure Sockets Layer
DR	Disaster Recovery

If you need any further information, please contact: GAmbx@sds.co.uk

Contents

1. Graduate Apprenticeships in Scotland

1.1 Purpose of the Graduate Apprenticeship framework document

The purpose of this document is to provide employers and learning providers with information required to deliver a Graduate Apprenticeship in **Cyber Security**. The framework sets out the skills and learning outcomes identified through employer consultation that are required to support the development of this programme.

This framework document should be read in conjunction with the following publications:

1. Work-based Learning Principles
2. Product Specification at **SCQF level 10**
3. Quality Assurance Guidance

This documentation is available on the Skills Development Scotland (SDS) corporate website:

www.skillsdevelopmentscotland.co.uk

1.2 What are Graduate Apprenticeships?

Graduate Apprenticeships (GAs):

- are accredited work-based learning programmes that lead to degrees or degree-level, professionally recognised qualifications
- are part of the apprenticeship family, supporting the transition into employment by providing work-based learning pathways from Foundation and Modern Apprenticeships to Higher and Graduate Apprenticeships, at SCQF Levels 8 –11
- have been developed as part of the Scottish Government's approach to developing Scotland's young workforce and Skills Development Scotland's work-based learning strategy

1.3 Why do we need Graduate Apprenticeships in Scotland?

International experience demonstrates how degree-level apprenticeships can drive economic growth. We believe this approach can benefit the Scottish economy.

The range of approaches taken in countries including Switzerland and Germany to develop employer-led, work-based learning pathways to learning and employment provide the basis for how Scotland can use work-based learning to improve the operation of the labour market and to deliver economic growth[1]. Skills Development Scotland is now leveraging the development of Graduate Apprenticeships to support this change.

[1] **PWC (2015) Young Workforce' Index: How well are OECD economies developing the economic potential of their young people?**

1.4 Who develops Graduate Apprenticeships?

Graduate Apprenticeships are developed by Skills Development Scotland through consultation with employers, universities, professional bodies and qualification authorities in the form of Technical Expert Groups (TEGs). The TEGs act as advisory groups on behalf of the sector and are based on the current and future skills needs of industry. They advise on the topics and related outcomes that should be included in a framework.

More information about who was involved in the development of this framework can be found in **Appendix C**.

1.5 Who are Graduate Apprenticeships for?

Graduate Apprenticeships provide a new way into degree-level study for individuals who are either currently in employment or are entering into employment. GAs are available to employees aged 16 or over.

1.6 Who delivers Graduate Apprenticeships?

Graduate Apprenticeships are delivered by universities in partnership with employers and college learning providers. An up-to-date list of learning providers and the frameworks they offer can be found on **www.apprenticeships.scot**.

2. Delivery

As Graduate Apprentices are work-based degrees, the place of employment is the place of learning. The learning and skills development must be fully integrated into both the **delivery and assessment** of the degrees when part of a Graduate Apprenticeship. This integration can only be satisfactorily achieved by proper planning and design prior to delivery and not by add-on components or ad-hoc modifications.

The authenticity of the programme is shown in the way employers are involved in the design and delivery of the degrees and the way in which work-based learning is positioned as integral to both the learning and the assessment needed for successful completion of the programmes.

GA are designed as full-time programmes. They are not part-time or sandwich courses. Attendance at the place of learning will be agreed between the provider and the employer sending individuals on the programmes. Examples of how this might work are:

- by day release or
- by block release of three or four-week duration, three times per year
- through distance learning with an initial “boot camp or induction”

Fundamentally, most of an individual’s time should be spent in the workplace on directed study.

Cyber Security (SCQF levels 10)

In designing the degrees to meet the work-based learning requirements of the GA, learning providers must ensure that they also meet the principles and criteria noted here:

Box 1. Principles and criteria

This GA is an SCQF level 10 work-based degree. All proposed university degree programmes for this GA framework must:

- be **480 credits**
- be based on a partnership between employers and the learning provider
- evidence how the programmes exemplify the work-based learning requirements
- have clear goals and aspirations in support of equality and diversity with appropriate monitoring and other processes in place
- demonstrate how they will ensure that apprentices, upon graduation, will consistently achieve the necessary industry skills, knowledge and competence defined in Appendix A
- develop learning through reflection and review of work processes and experience
- meet the requirements to apply for professional body recognition

NB Delivery models based on sandwich years or industrial placement block release are not considered as work-based learning as part of this framework.

The successful delivery of Graduate Apprenticeships depends upon an effective partnership between the apprentice, the employer and the learning provider. This will involve additions to their normal responsibilities for employees, learning providers, and apprentices.

Delivery of the content of the GA will be agreed by the participating learning providers, which may involve delivery of specialist or employer-specific content. Employers should also be closely involved with all aspects of the programme, including the course specification, delivery, and assessment of practical activities.

The learning provider has responsibility for the quality assurance and enhancement of all elements of the programmes but they must adhere to the SDS specified documents referenced in Section 1 and any additional guidance documentation provided as part of their competitive grant award. Practical activities must make use of the work environment and course content must take account of the technologies used in the apprentice’s employment.

Apprentices must have individual learning and training plans. The learning provider and existing employer HR systems should be co-ordinated during the development of the individual learning and training plan to ensure that the required employer contextualisation is effective. Even within a specific employer, there may be apprentices who use differing technologies.

3. Roles and responsibilities

3.1 Role of the employer

Apprentices are employees and subject to the standard terms and conditions applying to all employees.

Employers participating in the Graduate Apprenticeship programme must:

- consider whether a candidate has a reasonable chance of achieving the chosen programme during the selection process – this includes not only the course content but the acquisition of wider graduate attributes
- provide agreed information to support the candidate's application to the degree course
- provide apprentices with suitable opportunities to gain the type of experience in the workplace that will support their learning and skills acquisition
- provide each apprentice with a nominated mentor who must be readily accessible to the apprentice and to the learning provider
- liaise with the learning provider on the content and practical activities in the apprentice's individual learning and training plan
- provide information that will support the individual apprentice and their assessment

3.2 Role of the learning provider

Apprentices are both employed by the employer, as well as enrolled with the learning provider. As such they should have access to the same facilities as any other student.

GA course design and delivery must adhere to the principles detailed in preceding sections and in addition the learning provider must:

- adopt a flexible approach to considering the suitability of candidates by taking account of the portfolio of previous learning and experience an individual brings to the programme – this will include any relevant Foundation or Modern Apprenticeship undertaken – and support best practice in assessing individuals and in gathering evidence from employers where this is required
- liaise with the employer on the content and practical activities in the apprentice's individual learning plan

In addition, the learning provider should liaise with existing employer Training and Development and Quality Assurance (QA) systems to minimise double assessment. Development and meaningful implementation of individual learning plans is an essential component of the GA and assessments should take account of existing evidence wherever possible.

New evidence that directly relates to the workplace may be authenticated by employers or the individual's mentor.

There are a range of different delivery mechanisms, but the integration of knowledge within contextualised learning opportunities must be the overriding factor.

3.3 Content delivery and assessment

Content delivery and assessment responsibilities:

	Employer	***Learning Provider***	***Other***
Delivery of knowledge and understanding content	✓ Employer specific topics	✓ Generic and non-employer specific	✓ Private providers
Assessment of practical application	✓	✓	✓ Apprentice
Development of personal and business skills	✓ Specification, delivery, progress monitoring, assessment and mentoring	✓ Specification, delivery, progress monitoring and assessment	✓ May be a third party used for delivery, monitoring and assessment

4. Entry

4.1 Eligibility

- Graduate Apprenticeships are available to new and existing employees of participating employers.
- Candidates must be at least 16 years of age. However, the suitability of an individual for entry onto a GA will be decided by the employer and their learning provider partner.
- Candidates must be resident in Scotland throughout the Graduate Apprenticeship. In addition to this, their employer’s working premises must also be located in Scotland. When applying to become a Graduate Apprentice the individual will be required to satisfy the employer that they have the right to live and work in the UK.
- Entry requirements are likely to vary across learning providers. For courses where there is a mandatory requirement for a specific subject, learning providers should consider ways they can provide support to individuals who don’t hold a traditional qualification but have nevertheless shown aptitude and competence at the necessary level.

4.2 Recognition of prior learning

Candidates will undergo a selection process for a Graduate Apprenticeship, based on employer HR processes. The admissions departments need to take account of this and liaise with employers to provide advice and guidance on the prior learning and experience that will be accepted for entry onto the course.

A more flexible approach to entry requirements should be adopted by learning providers, and be done in consultation with employers. This should involve consideration of candidates on a case by case basis, who have completed relevant Foundation, Modern or Technical Apprenticeships as well as industry / vendor certifications.

Universities and other providers are asked to consider ways they can optimise the apprentice's prior learning within the programme to ensure there is no unnecessary repetition of content.

5. Demand[2]

This sector covers both the manufacture of hardware including computers, consumer electronics and telecommunication equipment and the development and publishing of software, web sites and data management activities. This is a fast paced sector where new job roles and competencies evolve quickly.

Employment[3]
In 2017, employment in the sector was 62,200 accounting for two per cent of all employment in Scotland. This makes it one of the smallest Key Sectors in Scotland measured by employment. Since the recession in 2008 employment in the sector has grown by 13 per cent, compared to a one per cent decline for all industries. More recently (since 2015) employment has declined by two per cent, compared to no growth across all industries. This suggests that despite being a relatively small key sector in terms of employment, it has been a source of jobs growth since the recession although recently there have been job losses.

The highest levels of employment were in Edinburgh, East and Midlothian (15,100) and GAsgow (12,600). There was a high concentration in West Lothian where employment in the sector was more than three times the national average. Employment in the sector was also above average in Fife, Edinburgh, East and Midlothian and the West Region. This suggests that although nationally the sector is small, there are a number of regions mostly in the central belt where the sector is an important source of jobs. Typically, rural factors and logistics have been barriers in the sector; however, technological developments are reducing the limitations of location and geography. Continued improvements in broadband and connectivity infrastructure will increase opportunities across Scotland.

[2] Source: Digital Scotland 'Scotland's Digital Technologies Summary Report' 2017 in conjunction with SDS, EKOSgen and Oxford Economics
[3] **Oxford Economics Regional and Sectoral Forecast (2000-27)**

Cyber Security (SCQF levels 10)

The recent employment decline in the sector is not forecast to continue. By 2020, employment in the sector will have increased by 1,400, an increase of two per cent. The growth is expected to continue over the longer term up to 2027, growing by seven per cent. This is more than double the rate of growth than all industries, which are expected to grow by three per cent. Growth will create jobs in the sector and the need to replace workers will also generate demand. Based on employment in 2017, six per cent of the workforce will need to be replaced by 2027. The sector's net requirement for workers up to 2027 will be 8,000. This is one per cent of the net requirement for workers across all industries.

In line with current employment, the greatest proportion of the total net requirements for workers in Digital Technologies sector will be located in Edinburgh, East and Midlothian (30 per cent); and GAsgow (20 per cent).

Occupations [4]

In 2017, the majority (66 per cent) of the Digital Technologies workforce were in higher level occupations. The proportion of the workforce in mid and lower level occupations was lower, 17 per cent each. In 2027 there will be a small change in the occupational structure of the workforce with two per cent more of the workforce being in higher level occupations and one per cent fewer in both mid and lower level occupations.

Graduates are most in demand by employers of technology staff, and those with technology, science and maths disciplines are most sought after. However 31% of graduates in technology roles do not have a computer science degree, representing the importance of transferable skills and aptitude and the willingness of employers to consider a range of career and learning pathways.[5]

Digital and Technology in Other Sectors[6]

Digital growth is no longer just consigned to Digital Technology companies as technology is now transforming and underpinning many sectors. Consequently there is increased demand for highly skilled individuals with technology skills to support the businesses. For example the increasing importance of technology within Financial Services has lead to the emergence of the sub-sector, Fintech, the amalgamation of Digital Technologies and Financial Services.

In 2016, 90,000 people were employed in technology roles across all sectors in Scotland; 60 per cent of these were in non-technology sectors. Technology occupations increased by 10 per cent from 2015 to 2016, and are forecast to continue to grow. Forecast demand, accounting for new and replacement demand, estimates 12,800 annual vacancies for technology roles in Scotland.

[4] Oxford Economics Regional and Sectoral Forecast (2000-27)

[5] Digital Scotland 'Scotland's Digital Technologies Summary Report 2017' in conjunction with SDS, EKOSgen, and Oxford Economics

[6] Digital Scotland 'Scotland's Digital Technologies Summary Report 2017' in conjunction with SDS, EKOSgen, and Oxford Economics

Cyber Security (SCQF levels 10)

The number of technology professionals employed in other sectors is growing faster than for technology businesses, further illustrating the demand for technology skills across all industries. This growth represents a significant opportunity for young people and other new entrants, but also means it is important that employers have a buoyant talent pipeline to support these vacancies.

Digital and ICT Skills Investment Plan

The Digital and ICT Skills Investment Plan (SIP) developed in 2014 identifies actions to support the growth ambitions of the sector. GAs could support a number of these actions including broadening the future talent pipeline for Digital Technology skills.

New Developments Influencing Demand for GAs

Cyber security is of growing importance as it cuts across all sectors underpinning virtually all technology innovations. The importance of getting cyber security right for Scotland is articulated in the Scottish Governments strategy Safe, Secure and Prosperous: A Cyber Resilience Strategy for Scotland.   Demand for cyber security skills has already risen by 70% since 2012, far greater than the growth in demand for technology professionals generally.[7]

Further policy and legislative changes such as the implementation of General Data Protection Regulation (GDPR) are likely to drive demand for skilled cyber security professionals.

The Scottish Government awarded SDS additional funding for cyber security careers events focusing on Work Based Learning (WBL) opportunities – as part of this, SDS has also committed to running industry events to raise awareness of GAs among employers (as well as MAs and FAs).

[7] Digital Scotland 'Scotland's Digital Technologies Summary Report 2017' in conjunction with SDS, EKOSgen, and Oxford Economics

6. The framework

6.1 Overview

The Cyber Security (CS) Graduate Apprenticeship is based on industry defined needs and has been developed in collaboration with employers and the education sector to allow knowledge, understanding, skills and competence to be developed with the necessary attributes industry expects from its graduates.

Within the CS Graduate Apprenticeship, the degree content must be delivered per the principles and outcomes detailed in this framework.

The specific Graduate Apprenticeship included in this framework is:

- **Cyber Security (CS)**

The output of this framework will be a Graduate Apprenticeship at **SCQF level 10** entitled:

Graduate Apprenticeship in BEng (Hons) Cyber Security

6.2 Purpose

The purpose of the Graduate Apprenticeship in **Cyber Security** is to produce graduates with a common core of skills and knowledge who can:

- Identify, analyse and evaluate security threats and hazards to a digital business system or service using relevant external sources of threat intelligence or advice (e.g. CERT UK).
- Research and investigate different attack techniques and recommend how to defend against them using relevant external sources of vulnerabilities (e.g. OWASP).
- Discover vulnerabilities in a digital system and undertake a security risk assessment, proposing remediation advice in the context of the employer.
- Develop a security case to describe the security objectives, identifying what threats, vulnerability or risks are mitigated through technical, implementation, policy or process aspects.
- Recommend and implement appropriate cyber security defences to defend against identified attack techniques.
- Understand the foundations of cyber security, its significance to business and society, the theory and concepts such as; security, identity, confidentiality, integrity, availability, threat, vulnerability, risk, hazard and assurance, and how these relate to each other.
- Understand information security assurance and how it may be achieved in practice, including the role of security testing (e.g. vulnerability and penetration testing).

Cyber Security (SCQF levels 10)

- Understand cyber security concepts applied to ICT infrastructure, including the fundamental building blocks and typical architectures of software applications, databases and networks, identifying common vulnerabilities in these different systems.
- Understand the range of different attack techniques and sources of threat, including the role of human behaviour and how attack techniques combine with motive and opportunity to become a threat.
- Apply and understand relevant laws and ethics – describe security standards, regulations and their consequences across at least two sectors; the role of criminal and other law; key relevant features of UK and international law.
- Understand the existing threat landscape, trends and their significance, including how to apply relevant techniques for threat intelligence.
- Ability to work confidently as an individual and as part of a team to develop and deliver cyber security deliverables
- Demonstrate the skills, knowledge and understanding of the need to embed cyber security resilience requirements throughout application and infrastructure development life cycles.

6.3 Occupational outcomes

7. The **Cyber Security** GA is aimed at employment in the following areas:

- Intrusion analysis
- Network security
- Information security governance
- Information security testing

The **Cyber Security** GA is aimed at high potential, mathematical, creative-thinking students who are interested in the design and development of software applications and systems. Alongside building technical aspects of complex software systems, the taught programme would cover team-working, personal / interpersonal, management and project skills spread across all roles that drive fundamental technologies of the world today.

Details of the high-level learning and skills outcomes for these content areas are provided in **Appendix A** along with some examples of low level learning outcomes in **Appendix B**.

Occupational outcomes

The **Cyber Security** GA is typically aimed at employment in the following areas:

- Cyber security analyst
- Malware analyst
- Security tester
- Security engineer
- Cyber security and information risk advisor
- Cyber security / information assurance architect
- Information security accreditor
- Cyber security / information assurance auditor
- IT / network security engineer
- Cyber security forensics analyst

6.4 Learning outcomes

Please refer to **Appendix A** for a full list of high level learning outcomes for the **Cyber Security** GA.

6.5 Professional recognition

The **Cyber Security** GA framework supports the achievement of professional recognition as relevant to the degree specified. The achievement of a degree as part of a GA, including the professional experience gained, and the completion of the work-based project, will provide the evidence of recognised accomplishment and acceptance as a full and professional practitioner in the IT industry through IEng recognition.

The UK Standard for Professional Competence (UKSPEC) sets out the competence and commitment required for registration as an Incorporated Engineer (IEng). The degrees that have been designed to be used within the **Cyber Security** GA include the range of learning and skills outcomes that demonstrate the required competence and commitment to achieve Incorporated Engineer (IEng) recognition. A candidate on completion of a GA will also be on course to demonstrate the requirements for Chartered Engineer (CEng) in the future.

Cyber Security (SCQF levels 10)

The following Scottish Apprenticeship frameworks and qualifications are relevant pathways that may contribute toward progression into the **Cyber Security** GA. The apprenticeships are eligible for funding contributions from Skills Development Scotland and provide individuals and employers with a range of alternative pathways at different levels of entry:

In school:

- Foundation Apprenticeship in ICT and Digital (SCQF level 6)

FA ICT and Digital SCQF L6

Post-school:

- Modern Apprenticeships in IT and Telecommunications (SCQF level 5)

MA IT and Telecommunications SCQF L5

- Technical Apprenticeship in Information Security (SCQF level 8)

TA Information Security SCQF L8

- Technical Apprenticeship IT and Telecommunications (SCQF Level 8)

TA IT and Telecommunications SCQF L8

Appendix A. Learning and skills outcomes

FRAMEWORK: Cyber Security (SCQF level 10)

This section details the high-level learning and skills outcomes for the GA in Cyber Security that must be covered within the degree.

This presents a broad set of outcomes against which universities can position their intended provision to meet the high-level learning outcomes and flavour the programme for their intended employer audience.

Topics and high-level learning and skills outcomes:

Learning and skills outcomes for Cyber Security (core)
1. Security concepts and foundations
1.1. Cyber security concepts
1.2. Cyber security threats
1.3. Cyber security vulnerabilities
1.4. Insider threat analysis and management
1.5. Information assurance
1.6. Cyber security culture
1.7. Cyber security awareness
2. Secure network and application infrastructures
2.1. Computer networks
2.2. Computer hardware
2.3. Cloud infrastructure
2.4. Operating System (OS) fundamentals
2.5. Programming, low level coding, scripting & principles of secure programming
2.6. Databases
2.7. System engineering principles and software development lifecycle
2.8. Cyber-physical systems
2.9. Practical security considerations
3. Threats, vulnerabilities, impacts and mitigations in ICT systems and the enterprise environment
3.1. Attack techniques, research and investigation
3.2. Threat and hazard identification, analysis and evaluation

3.3. Attack Prevention and mitigation against security threats and hazards
3.4. Malware analysis
3.5. Impact assessment
4. Intrusion detection, incident investigation and management, and digital forensics
4.1. Security monitoring, analysis and intrusion detection
4.2. Incident response management and handling
5. Risk assessment and management
5.1. Risk modelling and analysis
5.2. Risk assessment
5.3. Risk management
5.4. Developing a security case
6. Cyber security governance
6.1. The legal, regulatory and compliance environment
6.2. The role of assurance in management of the secure enterprise
6.3. Security management standards and policies
7. Personal and interpersonal
7.1. Communications
7.2. Personal attributes
7.3. Professional attributes
7.4. Team working

Learning and skills outcomes for Cyber Security (optional) pathways. Please select at least one of the following pathway options:
8. Security testing
8.1. Operating within a legal and ethical framework
8.2. Penetration testing
8.3. System reconnaissance and intelligence analysis
9. Digital forensics
9.1. Securing the scene
9.2. Forensic analysis of digital devices
9.3. Providing evidence
10. Security architecture
10.1. Architecting secure systems
10.2. Security technology and components
10.3. Human aspects and security usability
11. Information security audit and compliance
11.1. Internal and Statutory Audit
11.2. Compliance Monitoring
12. Malware research and reverse engineering
12.1. Malware research
12.2. Malware reverse engineering
13. Secure operations management
13.1. Secure operations management
13.2. Identity and access management
14. Business resilience
14.1. Business continuity
14.2. Disaster recovery

Appendix B. Low-level outcomes examples

The next section provides examples of low level learning and skills outcomes which employers may expect individuals to cover in a Graduate Apprenticeship in Cyber Security degree

The low-level learning and skills outcomes are not intended to be used as a pro-forma curriculum.

Each learning provider will have their own approach to delivering the degree and progression between stages. The low-level skills and derived learning outcomes that are detailed in the following sections will provide guidance to ensure that each degree covers the desired learning outcomes appropriately.

Table 1 Skills and knowledge coverage in security concepts and foundations

1. Security concepts and foundations
1.1. Cyber security concepts
1.2. Cyber security threats
1.3. Cyber security vulnerabilities
1.4. Insider threat analysis and management
1.5. Information assurance
1.6. Cyber security culture
1.7. Cyber security awareness

1.1 Cyber security concepts

CS1.1a Understand why cyber security matters – the importance to business and society, which includes the inclusion and significance of cyber security to critical and safety critical systems (including healthcare systems, critical national infrastructure, industrial plant automation, autonomous vehicles, mass transportation, internet of things).

CS1.1b Understand basic concepts: security, identity, confidentiality, integrity, availability, threat, vulnerability, impact, consequences risk and hazard and how these relate to each other and lead to risk and harm.

CS1.1c Explain how cyber security concepts apply to ICT infrastructure.

CS1.1d Describe attack techniques and sources of threat and the role of human behaviour. Explain how attack techniques combine with motive and opportunity to become a threat.

CS1.1e Understand the concept of an attack chain: how to put an attack into a larger (greater than one’s own organisation) context or as part of a more sophisticated attack.

CS1.1f Understand security assurance concepts (eg explain what assurance is and explain ‘trustworthy’ versus ‘trusted’) and how assurance may be achieved in practice (can explain what penetration testing is and how it contributes to assurance and extrinsic assurance methods).

CS1.1g Understand the theory and practice of cryptography, including; block ciphers, cryptographic hash functions, public key cryptography and cryptographic protocols.

1.2 Cyber security threats

CS1.2a Understand the existing threat landscape. Recognise how to apply relevant techniques for horizon scanning, including use of known sources of threat intelligence to keep the view of the threat landscape up to date.

CS1.2b Understand the nature of threat trends, how to identify these and the significance of identified trends.

CS1.2c Understand the threat intelligence lifecycle and the concepts of threat actors and attribution.

CS1.2d Understands the significance, value and limitations of a given threat analysis.

1.3 Cyber security vulnerabilities

CS1.3a Understand the fundamental building blocks and typical architectures in networks and systems and identify some common vulnerabilities.

CS1.3b Understand vulnerabilities in computer networks and systems (for example unsecure coding and unprotected networks) and how they can be exploited.

CS1.3c Identify the vulnerabilities in organisations security management system. Identify the links between physical, logical, personal and procedural security.

1.4 Insider threat analysis and management

CS1.4a Understand the nature of insider threats by an employee or contractor working within or on behalf of the company or organisation which could result in a potential security breach and potential access to and loss of data or other disruptive activity either maliciously or accidentally.

CS1.4b Understand the need for the rapid identification of the actions of a person who has either intentionally or mistakenly carried out a data breach so that this can be reported to management to both mitigate the impact of the data breach, identify the identity of the person who carried out the act and assess the potential impact of the data breach.

CS1.4c Understand the need for an organisation to define an Insider Threat Strategy that will include business, technical and operational requirements and objectives for an Insider Threat program framework that will manage insider threats.

1.5 Information assurance

CS1.5a In security, explain the difference between ‘trusted’ and ‘trustworthy’ and explain what assurance is for.

CS1.5b Understand the main approaches to assurance (intrinsic, extrinsic, design & implementation, operational policy & process) and how these might be applied at different stages in the lifecycle of a system.

CS1.5c Understand current systems of extrinsic assurance (e.g. red teaming, security testing, supply chain assurance, Common Criteria) including the benefits and limitations.

CS1.5d Understand what 3rd party testing (e.g. ‘ethical hacking’) is and how it contributes to assurance.

CS1.5e Understand the different ways an organisation can provide intrinsic assurance.

1.6 Cyber security culture

CS1.6a Understand the benefits of behavioural analysis and security culture management in maintaining good information security.

CS1.6b Explain the need for appropriate governance, organisational structure, roles, policies, standards and guidelines for cyber and information security and how they work together to deliver identified security outcomes.

CS1.6c Assess security culture using a recognised approach.

1.7 Cyber security awareness

CS1.7a Understand the role of information security awareness and training.

CS1.7b Understand the motivations and ways of thinking of different classes of threat actors, criminal intent, activism, state actors, hackers and how this drives the behaviour of the threat actors in order to understand how to tailor mitigations for the different classes of threat actor.

CS1.7c Understand the Insider Threat and the difference between malicious intent and human error.

CS1.7d Understand the need for ‘usable security’ in which security mechanisms are designed to consider the ways in which people work – i.e., the mechanisms are not too time consuming to use or so complex that people make mistakes or try to by-pass them.

Cyber Security (SCQF levels 10)

CS1.7e Design and implement a simple security awareness campaign to address a specific aspect of security culture.

CS1.7f Demonstrates good personal security hygiene appropriate to the employer context.

CS1.7g Develop authoritative awareness materials and undertake Information Security briefs to staff at all levels within the organisation.

CS1.7h Be able to brief the media on aspects of cyber security matters after seeking relevant approval from managers.

Table 2 Skills and knowledge coverage in secure network and application infrastructures

2. Secure network and application infrastructures
2.1. Computer networks
2.2. Computer hardware
2.3. Cloud infrastructure
2.4. Operating System (OS) fundamentals
2.5. Programming, low level coding, scripting and principles of secure programming
2.6. Databases
2.7. System engineering principles and software development lifecycle
2.8. Cyber-physical systems
2.9. Practical security considerations

2.1 Computer networks

CS2.1a Describe the fundamental building blocks (e.g. routers, switches, hubs, storage, transmission) and typical architectures (e.g. server/client, hub/spoke) of computers networks and the internet.

CS2.1b Explain what is meant by data and protocol and how they relate to each other. Describe an example data format and a simple protocol in current use (using protocol diagrams). Describe example failure modes in protocols, for example reasons why a protocol may ‘hang’ and the effect on a protocol of data communication errors. Describe at least one approach to error control in a network.

CS2.1c Describe the main features of network protocols in widespread use on the internet and their purpose and relationship to each other, including the physical and data link layer (e.g. https, HTTP, SMTP, SNMP, TCP, IP, BGP, DNS etc.).

CS2.1d Understand the main routing protocols in current use in computer networks and explain the differences between static and dynamic routing protocols and the pros and cons of each in different circumstances

CS2.1e Understand the main factors that affect network performance (e.g. the relationship between bandwidth, number of users, nature of traffic, contention) and methods that can be applied to improve performance (e.g. application of traffic shaping, changes to architecture to avoid bottlenecks and network policy that prohibit streaming protocols).

CS2.1f Understand the principles of network-based attacks: eavesdropping / sniffing, man-in-the-middle, spoofing, session hijacking, denial of service, traffic redirection, routing attacks, traffic analysis and malware.

CS2.1g Understand the security issues that may arise in the day to day operation of networks.

2.2 Computer hardware

CS2.2a The Apprentice should understand:

- classical computer architectures;
- virtualised architectures;
- digital logic, static and dynamic digital systems;
- machine level representation of data;
- assembly level machine organisation;
- memory system organisation and architecture;
- Interfacing and communication.

2.3 Cloud infrastructure

CS2.3a Recognise the impact of the employment of virtualisation techniques to networks and its role in 'Cloud'.

CS2.3b Understand the characteristics of cloud services from a business perspective.

CS2.3c Understand the key concepts of cloud implementation and digital asset migration.

CS2.3d Understand how to implement cloud performance monitoring systems.

CS2.3e Understand the application of security controls to cloud environments.

2.4 Operating System fundamentals

CS2.4a Understand that an OS defines an abstraction of hardware and manages resource sharing among a computer's users (all 2):

- OS principles;
- concurrency and synchronisation;
- scheduling and dispatch;
- memory management;
- security and protection;
- kernel security and protection;
- file systems;
- I/O system.

CS2.4b Understand typical OS security features and how these may themselves be exploited.

2.5 Programming, low level coding and scripting and principles of secure programming

CS2.5a Understand:

- algorithms and program design;
- fundamental programming concepts;
- fundamental data structures, and
- typical program development environment and methods.

CS2.5b Understand that programming languages are the medium through which programmers precisely define concepts, formulate algorithms and reason about solutions including:

- functional programming;
- event driven and reactive programming;
- language translation and execution;
- syntax analysis;
- compiler semantic analysis;
- code generation;
- coding in assembler;
- machine code;
- scripting language, and
- object-oriented programming

2.6 Databases

CS2.6a Understands basic information management concepts, including:

- information storage and retrieval;
- information capture and representation, and
- searching, retrieving, linking, and navigating.

CS2.6b Understand database concepts, including:

- components of database systems;
- design of core DBMS functions (e.g. query mechanisms, access methods), and
- database architecture and query language.

2.7 System engineering principles and software development lifecycle

CS2.7a Understand how the different aspects in a software development lifecycle combine to deliver a successful outcome by considering; meeting a need, design, trade-offs, implementation, deployment, support, evolution, validation, verification and assurance.

CS2.7b Can describe different approaches to developing software, including sequential and iterative/agile approaches.

CS2.7c Can explain the advantages and disadvantages of different software development processes and justify choice of process in different contexts.

CS2.7d Understand how to select and use different tools and environments that support software development at different stages in the lifecycle.

CS2.7e Understand principles of systems engineering, including all aspects of technology, people, culture and process and the environment within which a system of interest exists and operates.

CS2.7f Understand the benefits of a system approach to deal with challenges arising from complexity, emergence, adaptation and co-evolution.

2.8 Cyber-physical systems

CS2.8a Understand how software can interact with the hardware/physical environment, by describing:

- how software running on a microprocessor may interact with signals from sensors or effect actuators;
- how to identify a threat actor may exploit the external environment or software/hardware interface and mitigations that may be employed.

CS2.8b Understand the specific security challenges posed by ‘embedded systems’ (i.e. with size, power, processor, memory, scale and bandwidth limitations) e.g. ‘Internet of Things’ (IoT) devices.

2.9 Practical security considerations

CS2.9a Understand how classic security components including firewalls, proxies, network intrusion detection systems (NIDS), host-based intrusion detection systems (HIDS), intrusion prevention system (IPS) network zoning and physical and virtual device hardening can contribute to improving security resilience.

CS2.9b Understanding security within virtual environments including Cloud hardening, atomic host and use of containers.

CS2.9c Understand the role of security products such as NIDS, HIDS and IPS and how to apply them.

CS2.9d Understand how to apply standard secure configurations to fully harden any device placed on a secure network.

Table 3 Skills and knowledge coverage in threats, vulnerabilities impacts and mitigation in ICT systems and the enterprise environment

3. Threats, vulnerabilities, impacts and mitigations in ICT systems and the enterprise environment
3.1. Attack techniques, threat intelligence research and investigation
3.2. Threat and hazard identification, analysis and evaluation
3.3. Attack prevention and mitigation against security threats and hazards
3.4. Malware Analysis
3.5. Impact assessment

3.1 Attack techniques, threat intelligence research and investigation

CS3.1a Research and investigate common and complex attack techniques including making use of relevant external and open sources of vulnerabilities, threat intelligence and advice e.g. a national cyber authority, OWASP.

CS3.1b Work with external intelligence providers to obtain technical details of attacks to proactively protect the organisation and where relevant, its customers.

CS3.1c Understand the human dimension of cyber security, the risk from insider threats and the need to adopt an adversarial thinking approach to system development and analysis. Analyse how an employee may enable a successful attack chain without realising it. Describe some things that may increase or decrease risks related to an organisation's 'cyber culture'.

CS3.1d Research, analyse and evaluate security threats and hazards to a specific system or service or processes.

CS3.1e Identify linked cyber-attack campaigns and identify the threat actors behind them.

CS3.1f Describe ways to defend against cyber-attack techniques.

CS3.1g Combine different sources to create an enriched view.

CS3.1h Demonstrate application of attack techniques in a lab setting (in a legal and ethical manner).

CS3.1i Devise mitigations to defend against security threats and hazards to a specific system or service or processes.

3.2 Threat and hazard identification, analysis and evaluation

CS3.2a Understand the principles of threat intelligence, modelling, analysis and assessment.

CS3.2b Prioritise threats to an organisation and their methods of attack.

CS3.2c Analyse the significance and implication of processed intelligence to identify significant trends, potential threat agents and their capabilities.

CS3.2d Develop and implement threat monitoring use cases, derived from appropriate threat intelligence sources.

CS3.2e Assess efficiency and effectiveness of threat monitoring rules by adapting to the changing threat landscape and technologies.

3.3 Attack prevention and mitigation against security threats and hazards

CS3.3a Devise mitigations to defend against security threats and hazards to a specific system or service or processes.

CS3.3b Assist with investigations to identify and prevent cyber-attacks including those resulting from identifying new threats.

3.4 Malware Analysis

CS3.4a Understand the low-level mechanisms used by current malware, including:

- machine level instruction set;
- de-obfuscation of obfuscated code and
- anti-debugging mechanisms.

CS3.4b Analyse examples of malware and identify the mechanisms used by the malware.

3.5 Impact assessment

CS3.5a Understand the potential impact of poor Information Security and the business benefits of Information Security

CS3.5b Understand the impact of identified vulnerabilities in the organisation’s context.

Table 4 Skills and knowledge coverage in intrusion, detection, incident investigation and management

4. Intrusion detection, incident investigation and management
4.1. Security monitoring, analysis and intrusion detection
4.2. Incident response management and handling
4.3. Digital Forensics

4.1 Security monitoring, analysis and intrusion detection

CS4.1a Understand network monitoring and logging techniques and technologies.

CS4.1b Understand how attack techniques and vulnerabilities manifest in network monitoring and logging systems so that (for example) analysis of a network log or the output of a network monitoring tool may reveal the likely means of an attack.

CS4.1c Understand the relative merits of manual and automated techniques.

CS4.1d Understand the relative merits of signature based anomaly detection and algorithmic anomaly detection.

CS4.1e Understand how statistical techniques might be applied in support of analysis of cyber security incidents.

CS4.1f Recognise anomalies in observed network data structures (including by inspection of network packet data structures) and network behaviours (including by inspection of protocol behaviours) and by inspection of log files

CS4.1g Monitor automated tools including SIEM (Security Information Event Management) toolsets, investigate alerts and carry out configuration changes to improve performance.

CS4.1h Integrate and correlate information from various sources (including log files from different sources, network monitoring tools, SIEM tools, access control systems, physical security systems) and compare to known threat and vulnerability data to form a judgement based on evidence with reasoning that the anomaly represents a network security breach.

CS4.1i Characterise an anomaly in terms of its potential impact on the organisation.

4.2 Incident response management and handling

CS4.2a Understand and advise others on cyber incident response processes, incident management processes and evidence collection/preservation requirements to support incident investigation.

CS4.2b Understand how to communicate effectively with the incident response team/process and/or customer or other external authority incident response team/process for incidents.

CS4.2c Manage local response to non-major incidents in accordance with a defined procedure.

CS4.2d Interact and communicate effectively with the incident response team/process and/or customer or other external incident response team/process for incidents.

CS4.2e Organise cyber security incident investigation work within a legal and ethical framework (under UK jurisdiction).

CS4.2f Investigate and resolve incident records in line with business requirements.

CS4.2g Produce and document appropriate detection, containment and response strategies and processes in accordance to business requirements.

4.3 Digital Forensics

CS4.3a Understand principles of computer forensics and security, including evidential processing and an overview of basic analysis techniques.

CS4.3b Understand the fundamentals of detection, acquisition, analysis and digital forensic report writing.

CS4.3c Understand the legal and professional issues relating to the practice of obtaining ‘legally safe’ evidence of criminal activity

Table 5 Skills and knowledge coverage in risk assessment and management

5. Risk assessment and management
5.1. Risk modelling and analysis
5.2. Risk assessment
5.3. Risk management
5.4. Developing a security case

5.1 Risk modelling and analysis

CS5.1a Understand:

- asset valuation and management concepts;
- risk analysis methodologies in common use;
- risk appetite and risk tolerance concepts;
- economics of security concepts;
- different ways of treating risk (mitigate, transfer, accept etc.);
- principles of system risk modelling, and
- a system risk modelling methodology.

CS5.1b Apply system modelling techniques to risk, vulnerability and impact in order to enable trade-offs and to inform risk analysis. Employ a method such as SABSA, DBSY, CVSS scoring, STRIDE, NIST 800-154.

CS5.1c The ability to compose a system to create an architectural model for the purpose of risk assessment. Have the capability to integrate with an enterprise model.

5.2 Risk assessment

CS5.2a Understand risk assessment methodologies and different approaches to risk treatment (mitigate, transfer, accept, etc.)

CS5.2b Understand that risks may be described in qualitative, quantitative terms or some combination thereof.

CS5.2c Understand the role of the risk owner and contrast that role with other stakeholders.

CS5.2d Undertake a security risk assessment for a simple system without direct supervision and propose basic remediation advice in the context of the employer.

CS5.2e Conduct a cyber-risk assessment against an externally (market) recognised cyber security standard using a recognised risk assessment methodology.

5.3 Risk management

CS5.3a Understand the principles of information security risk management.

CS5.3b Develop Cyber and Information Security risk management strategies and controls, consider business needs and risk assessments and balance technical, physical, procedural and personnel controls.

5.4 Developing a security case

CS5.4a Understand the importance of developing a financial case for cyber security and how good cyber and information security strategies and processes can benefit the business.

CS5.4b Relate cyber security risk to other relevant classes of risk (business and operational risks) and perform costs analysis and present trade-off arguments in a business case, illustrating commercial or value for money judgement.

CS5.4c Compose a security case, deriving security objectives with reasoned justification in a representative business scenario.

CS5.4d Understand how to develop and implement a security improvement plan for the organisation’s overall security posture.

Table 6 Skills and knowledge coverage in cyber security governance

6. Cyber security governance
6.1. The legal, regulatory and compliance environment
6.2. The role of assurance in management of the secure enterprise
6.3. Security management standards and policies

6.1 The legal, regulatory and compliance environment

CS6.1a Understand the key features of the main laws applicable to the UK that are relevant to cyber security issues (including legal requirements that affect individuals and organisations), e.g. Computer Misuse Act, Data Protection Act, General Data Protection Regulation (GDPR) and the Human Rights Act.

CS6.1b Understand the cyber security standards and regulations and their consequences for relevant sectors (e.g. Government, finance, telecommunications, petrochemical/process control).

CS6.1c Describe the implications of international laws and regulations that affect organisations, systems and users in the UK, movement of data and equipment across international borders and between jurisdictions (e.g. Digital Millennium Act, ITAR, Safe Harbour).

CS6.1d Describe the legal issues relevant to cryptography (UK, EU and US export control of cryptography and the Wassenaar Arrangement).

CS6.1e Explain the benefits and costs and the main motives for uptake of significant security standards such as Common Criteria, PCI-DSS, FIPS-140-2, Government (e.g. UK NCSC) schemes.

6.2 The role of assurance in management of the secure enterprise

CS6.2a Explain the difference between ‘trusted’ and ‘trustworthy’ and explain what assurance is for in security.

CS6.2b Describe the main approaches to assurance (intrinsic, extrinsic, design and implementation, operational policy and process) and give examples of how these might be applied at different stages in the lifecycle of a system.

CS6.2c Understand different systems of extrinsic assurance (e.g. red teaming, security testing, supply chain assurance, Common Criteria) explaining the benefits and limitations.

CS6.2d Understand what 3rd party testing (e.g. ‘ethical hacking’) is and how it contributes to assurance.

CS6.2e Understand the different ways an organisation can provide intrinsic assurance.

6.3 Security management standards and policies

CS6.3a Explain the key concepts and benefits of applying an information security management system by reference to an internationally recognised standard (ISO27001, or similar).

CS6.3b Explain the need for appropriate governance, organisational structure, roles, policies, standards and guidelines for cyber and information security and how they work together to deliver identified security outcomes.

CS6.3c Explain how an organisation's security policies, standards and governance are supported by provisioning and access rights (e.g. how identity and access management are implemented and maintained for a database, application or physical access control system).

CS6.3d Describe how cyber security policies and procedures are used in different organisational environments and affect individuals and organisations.

CS6.3e Contribute to the effective operation of information security through the provision of system, policy and procedural advice to the business and 3rd party partners and suppliers

Table 7 Skills and knowledge coverage in personal and interpersonal

7. Personal and interpersonal
7.1. Communications
7.2. Personal attributes
7.3. Professional attributes
7.4. Team working

7.1 Communications

CS7.1a Identify the purpose of the communication, the audience and the outcomes to be achieved. Decide which method of communication to use and the level of formality required.

CS7.1b Make concise, engaging and well-structured verbal presentations, arguments and explanations of varying lengths, with and without the use of media always considering the audience viewpoint.

CS7.1c Competent in active listening, appreciating others views and contributions.

CS7.1d Give and receive feedback constructively by applying appropriate techniques and incorporate it into his or her own development and life-long learning.

CS7.1e Effectively prepare and deliver presentations using relevant presentation media products and the use of appropriate visualisations and images to present information and ideas clearly and convincingly.

CS7.1f Be fluent in written communications with the ability to articulate complex issues, selecting an appropriate structure and with appropriate tone, style and language.

CS7.1g Be competent at selling, questioning, negotiating and closing techniques in a range of interactions and engagements, both with internal and external stakeholders.

CS7.1h Prepare for and chair effective meetings with clear agendas and defined outcomes, keeping to time and preparing clear outcomes or ‘meeting minutes’ in a timely manner.

CS7.1i Produce clear and consistent technical documentation using standard templates.

7.2 Personal attributes

CS7.2a Be creative, self-motivated, self-aware and able to reflect on successes and failures in ways that strengthen positive attitude and develop self-reliance through an understanding of their own personal preferences, styles, strengths and weaknesses.

CS7.2b Can identify the preferences, motivations, strengths and limitations of other people and apply these insights to work more effectively with and to motivate others.

CS7.2c Can understand the outputs from and apply insights by using personal profiling tools such as Myers Briggs Type Indicator or Kirton Adaption/Innovation Indicator.

CS7.2d Can put forward, demonstrate value and gain commitment to a moderately complex technology-oriented solution, demonstrating understanding of business need, using open questions and summarising skills and basic negotiating skills.

CS7.2e Apply analytical and critical thinking skills to Technology Solutions development and to systematically analyse and apply structured problem solving techniques to them.

7.3 Professional attributes

CS7.3a Capability to deal with different, competing interests within and outside the organisation with excellent negotiation skills.

CS7.3b Deal with discord and confrontation including conducting difficult conversations

CS7.3c Conduct effective research using literature and other media into cyber security related topics.

CS7.3d Gather information from people using a variety of techniques including interviewing.

CS7.3e Understand the purpose of performance evaluation tools (including 360-degree feedback).

CS7.3f Understand the importance of learning strategies and techniques in own development, life-long learning and for corporate learning and development.

CS7.3g Understand the principles of personal development planning and create, implement and maintain a personal development portfolio and a personal action plan.

CS7.3h Understand the importance of acting with personal and professional integrity while always remaining focused and disciplined...

CS7.3i Plan and maintain own schedule with overall priorities assigned by a senior manager.

CS7.3j Within a dedicated timescale, deliver assigned tasks to the specified quality level and assist in quality assuring work of others if required.

CS7.3k Manage and maintain relationships with personnel both within the organisation and 3rd party partners ensuring correct completion of relevant technical and process security related documentation.

CS7.3l Be aware of various content that may be encountered in the employment of a cyber security related role.

CS7.3m Can apply personal resilience in own role and seek help and guidance from managers where appropriate.

7.4 Team-working

CS7.4a Plan and implement own work goals, objectives, priorities and responsibilities with others.

CS7.4b Understand how to motivate others and get the best from people.

CS7.4c Within the team, communicate, identify different abilities and potential and show respect for individuals.

CS7.4d Understand how high performing teams work effectively to produce cyber security solutions, work with team members to identify and solve problems and disagreements, share feedback with others on the achievement of team objectives and making promoting improving team-working.

CS7.4e Understanding of the importance of applying effective work habits, and leadership, providing clarity, direction and accountability and proactively acting when necessary.

CS7.4f Provide security related technical guidance to peers and junior staff members.

Learning and skills outcomes for Cyber Security (optional pathways)

Table 8 Skills and knowledge coverage in security testing

8. Security testing
8.1. Operating within a legal and ethical framework
8.2. Penetration testing
8.3. System reconnaissance and intelligence analysis

8.1 Operating within a legal and ethical framework

CS8.1a Understand the applicability of laws and regulations to carry out security testing of 3rd parties ('ethical hacking', 'pen-testing').

CS8.1b Reference and describe at least 1 generally recognised and relevant professional body that has ethical responsibilities as a cyber-security professional.

CS8.1c Understand the applicability of laws and regulation to gather intelligence collection and analysis and the relationship to data protection, human rights and privacy.

CS8.1d Organise cyber security testing work within a legal and ethical framework (under UK jurisdiction).

8.2 Penetration testing

CS8.2a Understand the principles, main components and the high-level processes involved in an infrastructure penetration test.

CS8.2b Scope and conduct vulnerability assessments and tests for weaknesses, assessing the potential for exploitation and where appropriate, by conducting exploits. Report potential issues and mitigation options.

CS8.2c Understand the principles of penetration testing against networks and infrastructures, web applications, mobile devices and control systems.

CS8.2d Design and implement test plans for penetration testing networks and application based information systems, to proactively target the most significant threats and vulnerabilities in line with organisational standards.

CS8.2e Identify and apply a range of appropriate methods, tools and techniques to conduct penetration testing for the identification of vulnerabilities for infrastructure and application contexts.

CS8.2f Perform infrastructure and application penetration tests, under controlled conditions, to assess compliance against relevant internal and/or external standards.

CS8.2g Accurately record and report on vulnerabilities and threats identified during penetration testing.

8.3 System reconnaissance and intelligence analysis

CS8.3a Understand how threat actors' actions appear in typical sources of information.

CS8.3b Understand how to source intelligence ethically so that it may be used as required.

CS8.3c Understand the principles of penetration testing against networks and infrastructures, web and other types of applications, mobile devices and control systems.

CS8.3d Understand methods an attacker/threat actor may use to build knowledge of a system they have limited or no direct access to, including:

- phishing
- exploiting an insider
- port scanning
- open source intelligence

Table 9 Skills and knowledge coverage in digital forensics

9. Digital forensics
9.1 Securing the scene
9.2 Forensic analysis of digital devices
9.3 Providing evidence

9.1 Securing the scene

CS9.1a Understand the basic principles and processes surrounding securing evidence.

CS9.1b Understand how to secure evidence appropriately to support legal proceedings including how to document a digital chain of custody.

CS9.1c Can assess the need for forensic activity.

CS9.1d Can coordinate forensic response activities and engage with the relevant organisational processes to ensure that forensic services are deployed appropriately.

CS9.1e Secure the scene and capture evidence in accordance with legal guidelines in the most effective manner to minimise disruption to the business. Maintain evidential weight, using specialist equipment as appropriate.

9.2 Forensic analysis of digital evidence

CS9.2a Understand the purpose of a digital forensic examination.

CS9.2b Analyse various digital device types including phones and computers for evidence.

CS9.2c Understand the range of industry standard digital forensic tools and techniques and how to apply them.

CS9.2d Secure evidence appropriately to support legal proceedings.

CS9.2e Understand how to analyse accounting and audit logs generated by IT systems for signs of suspicious or malicious behaviour.

CS9.2f Understand the need to remain conversant with advances in digital technologies.

9.3 Providing evidence

CS9.3a Analyse the evidence obtained to identify breaches of policy, regulation or law, including the presence of malware.

CS9.3b Understand how to specify the requirements to prepare a digital forensic laboratory and carry out laboratory tests and/or calibrations, including sampling, relating to appropriate industry standards.

CS9.3c Document and present evidence as appropriate, including preparing comprehensive technical reports and documents on findings in accordance with forensic regulations and relevant industry standards.

CS9.3d Provide written and oral evidence and act as a competent witness if necessary, which might include appearing at court of law.

Table 20 Skills and knowledge coverage in security architecture

10. Security architecture
10.1. Architecting secure systems
10.2. Security technology and components
10.3. Human aspects and security usability

10.1 Architecting secure systems

CS10.1a Describe the fundamental security technology building blocks and typical architectures and architecture frameworks.

CS10.1b Understand the design principles for architecting a secure system (including separation of concerns, fail-safe/fail-secure, defence in depth, least privilege, how to apply proven security architectural patterns from reputable sources and how to incorporate appropriate security controls).

CS10.1c Understand security assurance (‘trustworthy’ versus ‘trusted’) and how an architecture may be assured.

CS10.1d Apply interpretation of a security policy and risk profiles to design secure architectural solutions that meet security objectives, mitigate the risks and conform to legislation in a representative business scenario.

CS10.1e Critically analyse secure architectural solutions and security controls against defined security objectives to assess how effectively risks are mitigated, legal requirements and business requirements are met.

10.2 Security technology and components

CS10.2a Understand common types of security hardware and software which are used to protect systems. e.g. firewalls, encryption for data at rest, encryption for communication, intrusion detection systems (IDS), intrusion protection systems (IPS), identity and access management (IDAM) tools, anti-virus (AV), web proxy, application firewalls, cross domain components, hardware security module and how each may be used to deliver risk mitigation or implement a security case.

CS10.2b Understand the main cryptographic techniques (e.g. symmetric, public key, secure hash, digital signing, block cipher etc.) and how to apply them.

CS10.2c Understand the significance of key management and the main features, benefits and limitations of symmetric and public key cryptosystems and the significance of entropy.

CS10.2d Understand the role of cryptographic techniques in a range of different systems (e.g. GSM, Chip&PIN, common hard disk encryption, TLS, SSL, privacy enforcing technology) and the practical issues introducing such into service and updating them.

CS10.2e Select and configure common security hardware and software components (including SIEM toolsets) to implement a given security policy.

CS10.2f Maintain tuning and revalidation tasks for existing threat monitoring rules to required standards.

CS10.2g Design a system employing a crypto to meet defined security objectives. Develop and implement a key management plan for the given scenario/system.

CS10.2h Develop a key management plan for a given scenario/system.

10.3 Human aspects and security usability

CS10.3a Understand human aspect of security, the role of human behaviour and the role cyber security plays within an organisation with regard to people and the human interface with digital systems and software.

CS10.3b Understand the principles of usability and the trade-offs among trustworthy computing properties, such as usability v security and accountability and privacy.

CS10.3c Understand how social engineering and phishing exploit human behaviour as means of attack.

CS10.3d Identify design aspects of systems and software to make them both usable and safe and to balance security and usability.

Table 13 Skills and knowledge coverage in audit and compliance

11. Audit and compliance
11.1. Internal and statutory audit
11.2. Compliance monitoring

11.1 Internal and statutory audit

CS11.1a Understand the main principles and processes involved in conducting an audit.

CS11.1b Conduct security audits under supervision and as part of a team, against agreed information security policies and standards.

CS11.1c Undertake audits of 3rd parties whom have authorised network access or whom data is shared with.

CS11.1d Ensure new 3rd parties are appropriately audited prior to service commencement.

CS11.1e Manage and maintain the cyber security audit diary and audit work schedule.

CS11.1f Prepare audit reports and technical documentation to verify that information systems and processes meet the defined security criteria (requirements or policy, standards and procedures).

11.2 Compliance monitoring

CS11.2a Implement processes to verify on-going conformance for security and/or legal and regulatory requirements.

CS11.2b Perform security compliance monitoring checks and/or controls testing exercises in accordance with an appropriate methodology against technical, physical, procedural and personnel controls.

CS11.2c Contribute to the ongoing development of information security systems, policies and procedures through their implementation, continuous review and identification of gaps or non-compliance.

Table 42 Skills and knowledge coverage in malware research and reverse engineering

12. Malware research and reverse engineering
12.1. Malware research
12.2. Malware reverse engineering

12.2 Malware research

CS12.1a Understand the principles of applied malware research in Information Security.

CS12.1b Conduct basic applied research, e.g. leading to the development of simple exploits or an assessment of an existing cryptographic algorithm.

CS12.1c Perform malware research, correlating with collected intelligence to build upon a larger knowledge base of tracked malware threat activity.

12.2 Malware reverse engineering

CS12.2a Understand the principles of malware reverse engineering including reverse engineering techniques for malware analysis.

CS12.2b Perform malware reverse-engineering to identify the “what”, “how” and “why” for given malware.

CS12.2c Competently reverse engineer malware in support incident response and threat intelligence requirements.

Table 53 Skills and knowledge coverage in secure operations management

13. Secure operations management
13.1. Secure operations management
13.2. Identity and access management

13.1 Secure operations management

CS13.1a Understand the main processes for managing the security of information systems.

CS13.1b Assist in creating processes for maintaining the security of information throughout its existence, including establishing and maintaining security operating systems in accordance with security policies, standards and procedures.

CS13.1c Assist in managing the implementation of information security programmes and co-ordinating security activities across the organisation.

13.2 Identity and access management

CS13.2a Understand what is meant by ‘identity and access management’ and how to implement it.

CS13.2b Understand that identity and access management systems can be used to initiate, capture, record and manage user identities and their related access permissions in an automated way.

CS13.2c Understand the main features of an identity and access management system that facilitates the management of electronic identities and access privileges.

CS13.2d Implement account provisioning processes to ensure that the creation of user accounts and access to software and data is in line with organisational policies and standards.

CS13.2e Use, identity and access management tools and methods to gain rights to information systems with different security requirements in line with organisational standards.

Table 64 Skills and knowledge coverage in business resilience

14. Business resilience
14.1. Business continuity
14.2. Disaster recovery planning

14.1 Business continuity

CS14.1a	Understand how business continuity contributes to information security.
CS14.1b	Understand the internal and external standards for business continuity including ISO and how to apply them.
CS14.1c	Undertake a business impact analysis for the outage of different information systems within the organisation in line with organisational standards.
CS14.1d	Implement information security related business continuity management processes and plans in line with organisational requirements.

14.2 Disaster recovery planning

CS14.2a	Understand how disaster recovery planning contributes to information security.
CS14.2b	Estimate recovery time for an information system, recovery point and maximum tolerable downtime in line with organisational standards.
CS14.2c	Contribute to defining the need for and the development of Disaster Recovery (DR) plans, processes or functions.
CS14.2d	Assist the design and implementation of programs to include policies, standards, guidelines, training programs and a viable quality assurance process for disaster recovery.
CS14.2e	Assist in the coordination and establishment of disaster recovery programs and business resumption planning across different platforms.

Appendix C Framework development summary

A GA framework sets out the required knowledge, skills and learning outcomes identified through employer and key partner consultation to support the delivery of a Graduate Apprenticeship programme. This is achieved through employer and key partner input to Technical Expert Groups (TEGs).

TEGs are short life working groups designed to act as an advisory group on behalf of the sector and contributes to the development and course design of a GA. TEGs are integral to the process of developing GAs that provide quality, consistency and relevance to industry.

Each TEG is made up of employers, professional or industry bodies, learning providers, and subject/technical experts from the related industry.

The following organisations were consulted in the development of this framework:

Cyber Security (SCQF level 10)

Employers	Learning providers	Qualification and industry bodies
BBC	Abertay University	The Tech Partnership
BT	Glasgow Caledonian University	
DXC	Glasgow Clyde College	
Lloyds Banking Group	Edinburgh Napier University	
Morgan Stanley	Robert Gordon University	
NHS	The Open University	
Police Scotland		
RBS		
Scottish Government		
Tesco Bank		
Cervello Consultants		

Skills Development Scotland

This framework is also available on the Skills Development Scotland corporate website:
www.skillsdevelopmentscotland.co.uk