Skills
Development
Scotland

Graduate Apprenticeships

framework document for

Cyber Security at SCQF level 11

October, 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	16.06.17
2.0	Full draft for TEG	TEG members	10.08.17
3.0	Draft revised following questionnaire	TEG members	28.09.17
4.0	Revised following TEG 2nd Oct	TEG members	06.10.17
Final	Final	TEG members	
5.0	Higher Apprenticeship reference	SDS	28.06.19

Terms and abbreviations

Term	Meaning
SDS	Skills Development Scotland
GA(s)	Graduate Apprenticeships(s) / Apprentice(s)
SCQF	Scottish Credit and Qualifications Framework
TEG	Technical Expert Group
QA	Quality Assurance
BSc	Bachelor of Science
MSc	Master of Science
IT	Information Technology
UKSPEC	UK Standard for Professional Competence
IEng	Incorporated Engineer
CEng	Chartered Engineer
ICT	Information and Communication Technology
SIP	Skills Investment Plan
GDPR	General Data Protection Regulation
ARO	Annualised Rate of Occurrence
SLE	Single Loss Expectancy
ALE	Annualised Loss Expectancy
DDOS	Distributed Denial of Service
RPO	Recovery Point Objective
MTD	Maximum Tolerable Downtime
RTO	Recovery Time Objective
SIEM	Security Information and Event Management

Contents

1. Graduate Apprenticeships in Scotland

1.1 Purpose of the Graduate Apprenticeships framework document

The purpose of this document is to provide employers and learning providers with information required to deliver a Graduate Apprenticeships 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 11**
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 Apprenticeships. 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.

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 11 work-based degree. All proposed university degree programmes for this GA framework must:

- be 180 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 Apprenticeships 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 Apprenticeships. 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 Apprenticeships, 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

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[2]
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.

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

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

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 [3]

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.[4]

Digital and Technology in Other Sectors[5]

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.

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.

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

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

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

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.[6]

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).

6. The framework

6.1 Overview

The **Cyber Security (CS)** Graduate Apprenticeships at SCQF level 11 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 Apprenticeships, the master's degree content must be delivered per the principles and outcomes detailed in this framework.

The specific Graduate Apprenticeships included in this framework is:

- **Cyber Security (CS)**

The output of this framework will be a Graduate Apprenticeships at **SCQF level 11** entitled:

Graduate Apprenticeships in BEng (Masters) Cyber Security

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

6.2 Purpose

The purpose of the Graduate Apprenticeships in **Cyber Security at SCQF level 11** is to produce post-graduates with a common core of skills and knowledge in either Information Security Assurance, Cyber Security Technology or Security Operations Centre:

An ***information security assurance specialist*** will:-

- Plan and lead cyber security audits, in accordance with organisational standards, designed to provide assessment of internal control processes and operational performance
- Identify security gaps and evaluate business risks using appropriate qualitative and quantitative methods
- Develop and implement a strong security awareness programme, promoting best practices and influencing a strong security aware culture
- Lead regular cyber security governance & compliance reviews to identify potential cyber security weaknesses and recommend improvements to mitigate/remove identified vulnerabilities and risks
- Plan and prepare cyber security audit communications, including audit reports and recommendations to strengthen internal cyber security controls
- Interprets information assurance and security policies and applies these to manage risks
- Provide advice and guidance to ensure adoption of and adherence to information assurance architectures, strategies, policies, standards and guidelines
- Maintain security administration processes and provide guidance in defining access rights and privileges
- Review and evaluate cyber security analysis and audit evidence prepared by team members for quality, and provide advice and guidance accordingly

A ***cyber security technical specialist*** will:-

- Assess security risks across a broad range of technical security solutions and designs
- Plan and carry out a variety of security testing strategies on IT infrastructures (wired and wireless), middle-ware and applications
- Research, analyse and evaluate technical threat intelligence to reduce cyber security threats and vulnerabilities
- Troubleshoot issues arising from vulnerability scanning
- Recommend cost-effective mitigations comprising careful combinations of technical, procedural and administrative controls

- Provide advice and guidance on the application and operation of elementary physical, procedural and technical security controls
- Perform security vulnerability assessments and testing and undertake business impact analysis for information systems
- Co-ordinate the planning of penetration tests, and deliver objective insights into the existence of vulnerabilities, and report on the effectiveness of defences and mitigating controls
- Plan and execute vulnerability and penetration tests, define and communicate the test strategy, manages test processes, and contributes to corporate cyber security testing standards
- Co-ordinate the execution of technical cyber security activities
- Select and apply tools and techniques to carry out a variety of testing strategies including penetration testing, fuzzy testing and ethical hacking.

A ***security operations centre specialist*** will

- Maintain a good understanding of evolving cyber threats to ensure the continued security of networks, including remaining up to date with current attack methods to identify threats and advise on prevention, mitigation and remediation;
- Prepare technical articles for internal knowledge base and participate in knowledge sharing with other SOC analysts and develop solutions efficiently;
- Perform real time network monitoring and packet analysis including monitoring, tuning, configuring and rule writing on Security Information and Event Management (SIEM) and other industry standard tools;
- Produce and maintain operational security processes and procedures;
- Perform triage on security events, raise incidents and support the incident management process;
- Analyse network, application and system log events in order to identify any potentially abnormal system behaviours and raise them as incidents for investigation.
- Work within prevailing change management processes to apply patches, provide 1st line support for supported security tools.

The **Cyber Security GA at SCQF level 11** 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.**

6.3 Occupational outcomes

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

- Information security audit, compliance and governance
- Cyber security testing, architecture, threat management or risk analysis and management
- Security operations centre (SOC)

6.4 Learning outcomes

Please refer to **Appendix A** for a full list of high level learning outcomes for the **Cyber Security GA at SCQF Level 11**.

6.5 Professional recognition

The **Cyber Security** GA framework supports the achievement of professional recognition as relevant to the master's degree specified. The achievement of a master's 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 master's 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.

6.6 Related Scottish apprenticeship frameworks

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:

Post school:

- Technical Apprenticeship in Information Security (SCQF level 8)

Technical Apprenticeship in IT SCQF L8

- Technical Apprenticeship in IT and Telecommunications (SCQF level 8)

Technical Apprenticeship in IT and Telecommunications SCQF L8

- GA in Cyber Security (SCQF level 10)

Graduate Apprenticeship Cyber Security at SCQF Level 10

Appendix A. Learning and skills outcomes

FRAMEWORK: Cyber Security (SCQF level 11)

This section details the high-level learning and skills outcomes for the GA in Cyber Security at SCQF Level 11 that must be covered within the master's 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.

Please note: all students will be expected to undertake a significant Cyber Security project at the end their course. This project should draw together all main skills of the course and include a real world applied design or manufacturing project.

Topics and high-level learning and skills outcomes:

The main core areas that are to be embedded are:

- Information and risk: including confidentiality, integrity and availability (CIA); concepts such as probability, consequence, harm, risk identification, assessment and mitigation; and the relationship between information and system risk.
- Threats and attacks: threats, how they materialise, typical attacks and how those attacks exploit vulnerabilities.
- Cyber security architecture and operations: physical and process controls that can be implemented across an organisation to reduce information and systems risk, identify and mitigate vulnerability, and ensure organisational compliance.
- Secure systems hardening and usability: the concepts of systems hardening and usability to ensure robust, resilient systems that are fit for purpose.
- Cyber security management: understanding the personal, organisational and legal/regulatory context in which information systems could be used, the risks of such use and the constraints (such as time, finance and people) that may affect how cyber security is implemented.
- Personal and professional: the ability to communicate, problem solve and work with and lead teams.

Plus, a specialisation optional pathway in one of the following areas:

- Information security audit and compliance
- Security testing
- Digital forensics
- Network security
- Secure operations

Topics and high-level learning and skills outcomes:

Learning and skills outcomes for Cyber Security (core)
1. Information and Risk
1.1. Information risk management as part of an organisation’s overall risk management
1.2. Risk landscape and threat categories
1.3. Residual risk
1.4. Risk management standards
1.5. Quantitative and qualitative approaches to risk management
2. Threats and attacks
2.1 Threats and threat intelligence
2.2. Vulnerabilities
2.3. Attack patterns and methodologies
2.4. Malware analysis and reverse engineering
3. Cyber security architecture and operations
3.1. Types of control
3.2. Incident handling, response and recovery
3.3. Principles of business/service continuity and disaster recovery as they relate to architecture and operations
3.4. Forensics and investigations
4. Secure systems hardening and usability
4.1. Systems hardening
4.2. Security usability
4.3. Designing for resilience
5. Cyber Security Management
5.1. Security and information assurance
5.2. Information security in the supply chain
5.3. Disaster recovery Business continuity management and plans
5.4. Resilience

6. Personal and Professional
6.1. Communications
6.2. Personal attributes
6.3. Professional attributes
6.4. Team working
Learning and skills outcomes for Cyber Security (optional pathways)
7. Information Security Audit and Compliance
7.1. Internal and Statutory Audit
7.2. Compliance Monitoring
8. Security Testing
8.1. Operate within an ethical and legal framework
8.2. Vulnerability assessment
8.3. Penetration testing
8.4. Countermeasures
9. Digital Forensics
9.1. Digital forensic concepts and principles
9.2. Digital Forensic tools and techniques
9.3. Digital Forensic analysis
9.4. Social, ethical and legal issues associated with digital forensics
10. Network Security
10.1. Secure network design
10.2. Secure network implementation and configuration
10.3. Secure network operations
11. Secure Operations
11.1. Security monitoring
11.2. Security event management
11.3. Operational security process management
11.4 Backup and restore management

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 Apprenticeships **in Cyber Security at SCQF level 11.**

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

Each learning provider will have its 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 information and risk

1. Information and Risk
1.1. Information risk management as part of an organisation's overall risk management
1.2. Risk landscape and threat categories
1.3. Residual risk
1.4. Risk management standards
1.5. Quantitative and qualitative approaches to risk management

CS1.1a Understand the concept of a risk landscape, its dynamic nature and how to create a landscape for an organisation

CS1.2a Can classify threats – and example categories system risk – its components and interactions with information risk

CS1.3a Understand the concept of residual risk and what it means for an organisation

CS1.4a Be aware of Risk management standards, such as: NIST SP800-30; Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE); CCTA Risk Analysis and Management Method (CRAMM); ISO 31000; ISO/IEC 27005

CS1.5a Understand that criteria can be used to assess the suitability of risk management approaches for an organisation, including quantitative approaches such as Annualised Rate of Occurrence (ARO), Single Loss Expectancy (SLE) & Annualised Loss Expectancy (ALE) and qualitative expressions of risk such as heat maps and Likert scales

Table 2 Skills and knowledge coverage in threats and attacks

2. Threats and Attacks
2.1 Threats and threat intelligence
2.2. Vulnerabilities
2.3. Attack patterns and methodologies
2.4. Malware analysis and reverse engineering

2.1 Threats

CS2.1a Understand:

- The difference between threat, risk, attack and vulnerability
- How threats materialise into attacks
- Where to find information about threats, vulnerabilities and attacks
- Typical threats, attacks and exploits and the motivations behind the
- That threats can materialise from insiders within the organisation
- How to classify threats

CS2.1b Understand the principles of threat intelligence, modelling and assessment, the range of modern attack techniques and how and where to research emerging attack techniques to inform the development of improved security controls, countermeasures and policies and standards.

CS2.1c Perform cyber threat intelligence analysis to research, analyse and evaluate technical threats by reviewing open source and other information from trusted sources for new vulnerabilities, malware, or other threats that have the potential to impact the organisation.

CS2.1d Understand the concept of a threat landscape, its dynamic nature and how to create a landscape for an organisation.

2.2 Vulnerabilities

CS2.2a Identify examples of cyber security vulnerabilities.

CS2.2b Perform a security vulnerability assessment for an organisation.

CS2.2c Maintain and manage software and hardware patching, particularly implementing vulnerability patching where vulnerabilities are identified.

2.3. Attack patterns and methodologies

CS2.3a Understand that there are different attacks, which have different patterns and different steps – for example can compare a Distributed Denial of Service (DDOS) to an attack designed to copy information.

CS2.3b Identify typical attacks (e.g. DDOS), phishing, buffer overflow and social engineering) and targets (e.g. people, databases, credentials).

CS2.3c Understand attack process and methodology (reconnaissance, scanning, creation, test, attack/gain access, exfiltration & exiting)/kill chain.

CS2.3d Understand that attacks can be combined for greater effect (e.g. phishing email, followed by social engineering phone call)

2.4. Malware analysis and reverse engineering

CS2.4a Understand that there are different types of malware – for example viruses, Trojans and spyware – their distribution mechanism and how they compromise information and systems.

CS2.4b Evaluate and demonstrate a critical and systematic understanding of malicious software and malicious code implementation.

CS2.4c Critically evaluate the design, code and the implementation of a malicious component and the steps required to reverse engineer the process.

CS2.4d Isolate an infected system and perform malicious code analysis and reverse engineering.

Table 3 Skills and knowledge coverage in cyber security, architecture and operations

3. Cyber security Architecture and Operations
3.1. Types of control
3.2. Incident handling, response and recovery
3.3. Business/service continuity and disaster recovery planning
3.4. Forensics and investigations

3.1 Types of control

CS3.1a Understand that cyber security controls can be categorised and selected based on that categorisation, and that they are used to align to areas of risk and to mitigate that risk.

CS3.1b Understand that where technical controls cannot be used, other controls can be selected.

CS3.1c Understand how technical controls (examples include cryptography, access management, firewalls, anti-virus software and intrusion prevention systems) work in detail/at an advanced level of understanding.

CS3.1d Understand how the technical controls can be deployed in practice – and associated strengths and weaknesses.

CS3.1e Be aware of the controls that can be used to mitigate against insider threats, including understanding who has access to critical systems and data, and implementing a process to detect and respond when out-of-policy actions occur.

CS3.1f Understand that the term “insider” is defined as a current or former employee, contractor, or business partner who has or had authorised access to the organisation’s network, systems, or data and that data breaches are accomplished via remote access to a company’s systems.

CS3.1g Understand the need to implement processes and controls that maintain the required level of security of a component, product, or system through its lifecycle and at end of life.

3.2 Incident handling, response and recovery

CS3.2a Understand how to develop and implement security event response programmes, security event handling, and operational security activities.

CS3.2b Understand the key steps in managing incidents and how to apply them.

CS3.2c Apply the organisations incident management process to ensure that incidents are handled appropriately.

3.3 Business/service continuity and disaster recovery planning

CS3.3a Understand the components and steps of a Business Continuity Plan/Disaster Recovery Plan (BCP/DRP) (e.g. ISO/ IEC 27031) and understand how to support BCP/ DRP measurement of recovery – Recovery Time Objective (RTO) /Recovery Point Objective (RPO)/ Maximum Tolerable Downtime (MTD).

3.4 Forensics and investigations

CS3.4a Understand the basic principles of digital forensics, including the principles and processes surrounding securing and analysing evidence, and recognises the capability of forensics to support investigations.

CS3.4b Understand that although encrypted data can be impenetrable at rest, it remains much more vulnerable on a live system and that live forensics can be used to obtain data when encryption is in use.

Table 4 Skills and knowledge coverage in secure systems, hardening and usability

4. Secure Systems Hardening and Usability
4.1. Systems hardening
4.2. Security usability

4.1 Systems hardening

CS4.1a Understand how security controls can be implemented to improve the protection of systems and information.

CS4.1b Understand how to apply a set of logical steps to harden servers and networks.

4.2 Security usability

CS4.2a Identify common trade-offs and compromises that are made in the design and development of security processes.

Table5 Skills and knowledge coverage in cyber security management

5. Cyber Security Management
5.1. Security and information assurance
5.2. Information security management systems
5.3. Privacy
5.4. Resilience

5.1 Security and information assurance

CS5.1a Understand the basic principles of information security governance and information assurance how it applies within an organisation.

CS5.1b Analyse the key components of an organisational cyber security strategy.

CS5.1c Compare different frameworks for cyber security management systems and standards such as ISO/IEC 27014 cyber security governance, ITGI Information Security Governance, the ISO/IEC 27036 series.

5.2 Information security management systems

CS5.2a Understand that ISO 27001 is a specification for an information security management system (ISMS). An ISMS is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organisation's information risk management processes.

CS5.2b Analyse the key components of an organisational cyber security strategy.

CS5.2c Compare different frameworks for cyber security management systems and standards such as ISO/IEC 27014 cyber security governance, ITGI Information Security Governance, the ISO/IEC 27036 series.

5.3 Privacy

CS5.3a Understand privacy as a special form of information protection, and that privacy and cyber security are linked.

CS5.3b Recognise that privacy has a legal and regulatory aspect, with obligations and requirements on individuals and organisations.

5.4 Resilience

CS5.4a Understand what resilience means, and how cyber resilience contributes to information security.

CS5.4b Understand the processes to anticipate, recognise and defend against changing Cyber and Information risk environments which threaten business stability.

CS5.4c Understand how to develop and implement plans to introduce a holistic culture of Information Security across an organisation aimed at identifying and reacting promptly and effectively to incidents.

Table 6 Skills and knowledge coverage in personal and professional

6. Personal and Professional
6.1. Communications
6.2. Personal attributes
6.3. Professional attributes
6.4. Team working

6.1 Communications

CS6.1a Develop and deliver management level presentations which resonate with senior stakeholders, both business and technical.

CS6.1b Professionally present cyber security plans and solutions in a well-structured business report.

6.2 Personal attributes

CS6.2a Demonstrate self-direction and originality in solving problems, and act autonomously in planning and implementing cyber security solutions at a professional level.

6.3 Professional attributes

CS6.3a Understand the strategic importance of cyber security processes, and how they are designed and managed to determine a firm’s security posture.

6.4 Team working

CS6.4a Develop own leadership style and professional values that contributes to building high performing teams.

CS6.4b Create strong positive relationships with team members to produce high performing technical teams.

Learning and skills outcomes for Cyber Security (optional pathways)

Table 7 Skills and knowledge coverage in information security, audit and compliance

7. Information Security Audit and Compliance
7.1. Internal, external and statutory audit
7.2. Compliance monitoring

7.1 Internal, external and statutory audit

CS7.1a Understand the main principles and processes involved in conducting an information security audit and how to apply them.

CS7.1b Plan and perform internal cyber security audits, using established audit methodologies to provide assurance that all activities are being carried out in accordance the written security policy and procedures.

CS7.1c Verify that information systems and processes meet the prescribed security criteria, identifying control weaknesses and suggesting process/control improvements.

CS7.1d Undertake audits of 3rd parties whom have authorised network access or whom data is shared with and ensure new 3rd parties are appropriately audited prior to service commencement.

CS7.1e Manage and maintain the cyber security audit diary and audit work schedule.

CS7.1f Plan and prepare cyber security audit communications, including audit reports and recommendations to strengthen internal cyber security controls.

CS7.1g Manage external audit activities, acting as point of contact for the external assessor as well as internal teams in the preparation for external audits as well as during the external audit itself.

7.2 Compliance monitoring

CS7.2a Can assess internal compliance against established security standards, including ISO27001, PCI-DSS and ND1643 Interconnect Standard and organisational security policies and processes & standards.

CS7.2b Carry out security compliance checks to ensure that services, processes and systems comply with organisational policies and legal requirements verifying that operationally these continue to ensure compliance.

CS7.2c Identify potential cyber security weaknesses and recommend improvements to mitigate/remove identified vulnerabilities and risks.

CS7.2d Can prepare a security compliance dashboard for discussion and review with senior managers.

CS7.2e Ensure that “insider vetting” processes are clearly defined and implemented to reduce insider threats.

Table 8 Skills and knowledge coverage in security testing

8. Security Testing
8.1. Operate within an ethical and legal framework
8.2. Vulnerability assessment
8.3. Penetration testing
8.4. Countermeasures

8.1 Operate within an ethical and legal framework

CS8.1a Understand the ethical and legal policies of security testing.

CS8.1b Operate according to the organisations ISO 27001 compliant information security management system.

8.2 Vulnerability assessment

CS8.2a Conduct vulnerability assessments and test for public domain vulnerabilities.

CS8.2b Assess the potential for exploitation, including by conducting exploits.

8.3 Penetration testing

CS8.3a Understand the principles, processes and tools involved in manual and automated penetration testing against networks and infrastructures, web applications, mobile devices and control systems.

CS8.3b Develop testing plans for infrastructure testing, application testing, scenario based testing, process testing, and social engineering.

CS8.3c Plan and carry out a variety of security testing strategies on IT infrastructures (fixed and wireless), middle-ware and applications, to discover vulnerabilities.

CS8.3d Develop pen testing reports which highlight and clearly articulate vulnerabilities and weaknesses to stakeholders.

8.4 Countermeasures

CS8.4a Develop appropriate remediation action plans and hardening plans and manage remediation of vulnerabilities.

CS8.4b Design and implement countermeasures to protect a network from unauthorised network access.

CS8.4c Recommend remediation and enhancements to security policies and information technology procedures

Table 9 Skills and knowledge coverage in digital forensics

9. Digital Forensics	
9.1.	Digital forensic concepts and principles
9.2.	Digital forensic tools and techniques
9.3.	Digital forensic analysis
9.4.	Social, ethical and legal issues associated with digital forensics

9.1 Digital forensic concepts and principles

CS9.1a Understand the concepts, principles, theories, challenges and techniques underpinning digital forensics and the maintenance of evidential integrity in all digital forensics.

9.2 Digital forensic tools and techniques

CS9.2a Understand the ways in which digital forensics tools and techniques can be applied to produce appropriate strategies and instigate change in an organisational and work based contexts in relation to digital forensics.

CS9.2b Understand the techniques, tools and issues involved in digital forensics investigations, including the limitations and constraints associated with those techniques.

9.3 Digital forensic analysis

CS9.3a Evaluate the application and validity of analytical methodology to digital forensic investigations.

CS9.3b Investigate digital artefacts against a brief, preserving, analysing and interpreting the evidence.

CS9.3c Report digital forensic findings to a non-specialist audience.

CS9.3d Apply scientific techniques and use scientific terminology appropriately in the context of digital forensic analysis.

9.4 Social, ethical and legal issues associated with digital forensics

CS9.4a Understand the professional, social, ethical and legal issues associated with digital forensics.

Table 20 Skills and knowledge coverage in network security

10. Network Security	
10.1.	Secure network design
10.2.	Secure network implementation and configuration
10.3.	Secure network operations

10.1 Secure network design

CS10.1a Have an advanced understanding of TCP/IP networking and networking technologies.

CS10.1b Can design and document secure, resilient and scalable networks, including VPN meshes, in a cloud-first implementation to produce security resilient platforms.

CS10.1c Can produce network diagrams and other technical documentation to support stakeholder review process.

CS10.1d Can produce high-level and low-level designs to support the migration of existing security technologies to bring into line with organisational standards.

CS10.1e Horizon-scanning for new risks and ensuring the network security controls remain relevant and effective.

CS10.1f Produce and maintain policies, procedures and documentation for network system security and ensure ongoing compliance.

10.2 Secure network implementation and configuration

CS10.2a Can install and maintain the operating system for network appliances including migrating to new OS release and patching.

CS10.2b Can configure a simple full-mesh VPN topology network.

CS10.2c Can maintain a software patching schedule.

CS10.2d Implement changes to ensure network systems meet business and technical requirements and follow enterprise architecture guidelines, technology standards and compliant with security standards.

10.3 Secure network operations

CS10.3a Can conduct a daily analysis of log files, intrusion reports, network statistics.

CS10.3b Can interpret and implement customer change requests on managed security device platforms, primarily firewalls and IDS/IDP devices.

CS10.3c Can run regular security scans, reviews and tests of the infrastructure.

CS10.3d Can remotely access and manage devices at various locations from a security operations centre.

CS10.3e Can extract existing rule sets from firewalls and convert these into an appropriate format for review.

CS10.3f Can perform a detailed analysis of existing rule sets to identify any rules which are redundant, do not meet the organisations security requirements or could be restructured to increase security.

Table 13 Skills and knowledge coverage in secure operations

11. Secure Operations
11.1. Security monitoring
11.2. Security event management
11.3. Operational security process management
11.4. Backup and restore management

11.1 Security monitoring

CS11.1a Can conduct a daily analysis of log files, intrusion reports, network statistics.

CS11.1b Maintain a good understanding of evolving cyber threats to ensure the continued security of networks, including remaining up to date with current attack methods to identify threats and advise on prevention, mitigation and remediation.

CS11.1c Perform real time network monitoring and packet analysis including using Security Information and Event Management (SIEM) and other industry standard tools.

CS11.1d Analyse security system logs, security tools, and available data sources on a regular basis to identify attacks against the enterprise and report on any irregularities, issues related to improper access patterns, trending, and event correlations and make suggestions for detection rules and system tuning.

CS11.1e Configure/tune SIEM alerts (including configuring and rule writing), managed firewalls and intrusion detection/prevention (IDS/IPS) systems.

11.2. Security event management

CS11.2a Respond to security events to determine appropriate actions.

CS11.2b Perform incident response activities and ensure that proper protection or corrective measures have been taken when an incident has been discovered.

CS11.2c Perform triage on security events, raise incidents and support the incident management process.

CS11.2d Investigate and analyse security events and alerts.

11.3. Operational security process management

CS11.3a Produce and maintain operational security processes and procedures.

CS11.3b Prepare technical articles for internal knowledge base and participate in knowledge sharing with other SOC analysts and develop solutions efficiently.

CS11.3c Work within prevailing change management processes to apply patches, provide 1st line support for supported security tools.

11.4. Backup and restore management

CS11.4a Understand that data can be lost, corrupted, compromised or stolen through hardware compromise, specific human activity, hacking and malware and that loss or corruption of data could result in significant business disruption.

CS11.4b Be able to identify what data is being backed up, the organisational backup schedule and periodically validating that data has been accurately backed up.

CS11.4c Produce and maintain operational security processes and procedures for data backup and restore.

.

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 Apprenticeships 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 11)

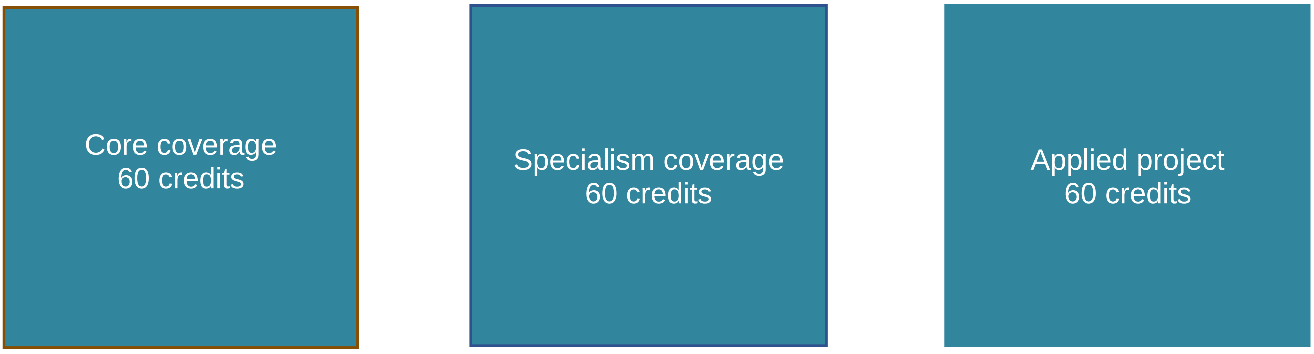
Employers	Learning providers	Qualification and industry bodies
BBC	Abertay University	The Tech Partnership
BT	Glasgow Caledonian University	
DXC	Glasgow Clyde College	
Lloyds Banking Group	Edinburgh Napier University	
Morgan Stanley	Robert Gordon University	
NHS		
Police Scotland		
Scottish Government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

Appendix D Progression Pathways into Cyber Security SCQF 11

Entry point	Core requirements for Level 11	Notes
First degree in computer science / software engineering / network engineering	May provide some coverage of infrastructure / applications elements of the core	In the majority of cases will require full core provision, but would depend upon architecture of the level 11 programme. But would seem sensible to adopt full core except exceptional circumstances.
First degree in cyber security topic	May provide some coverage of cyber security elements of the core	Much will depend upon the nature of the degree studied, the specialisation and final project. This may require a gap analysis, but again unlikely they have developed core outcomes in the context of the workplace
First degree in non-IT subject	Full core	Will require the full core delivery and may require additional bridging in IT principles. But a well-designed core design could provide most/all of the coverage required.
Existing employee with some relevant experience	Gap analysis against core	May provide exemption to some modules dependent upon nature of prior experience / academic and professional qualifications.
Apprentice successfully completing Level 10 GA in Cyber Security	In theory, should not be required to repeat the core unless there is level 11 differentiation of the core	In reality level 10 progression would not become possible until after four years. Thereafter they may become exempt through *APEL arrangements.

* APEL is the Accreditation of Prior Experiential Learning (APEL) and is the process for an applicant to seek formal recognition of prior learning they have achieved through experience or related qualifications when applying for a programme of study. In the case of a GA the university might normally state they require a certain number and grade of Scottish Highers. An employer might present a candidate who does not meet this but instead has related experience or different qualifications.

Possible generic architecture Level 11 MSc



Core coverage
60 credits

Specialism coverage
60 credits

Applied project
60 credits

Skills
Development
Scotland

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