Disciplines and Specialisms in Cyber Security

Purpose of this Paper

Introduction

This paper sets out to provide a high-level view on a potential way forward to identifying *Specialisms* for the UK Cyber Security Council (UK CSC). This paper describes some existing approaches already in use elsewhere, a proposed hierarchy specific to UK CSC, and then outlines a potential approach to implementation which will allow the Council to get to its goal of properly defining the professional requirements and (potential) registered status of its practitioners (including, but not limited to, Chartered status).

Specialisms in this paper are areas of expertise within the overall profession of Cyber Security. This high-level view recognises the differing and varied approaches taken by industry sectors, companies and organisations are very much dependent upon their size, structure and approach to cyber security.

There has been considerable debate over the terms *specialisms* and *disciplines* when trying to identify career pathways and to understand what *Skills* and *Roles* exist in the Information/Cyber security arena. For example, the security arena is fast changing, which reflects the ever-changing technology landscape and use and exploitation of information. As a further example, when cloud first appeared, many considered the knowledge to be a *Discipline*, but over time it has become just another body of knowledge which certain cyber practitioners need to acquire. Whatever approach is taken it must be flexible enough to be able to adapt to change with the developing field of cyber.

Although there is no agreed industry wide view of segmentation It is highly recommended the UK CSC build on existing resources and/or models to the extent possible to ensure both that we will be able to work with those models (when required) with the least possible effort and to avoid the unnecessary risks and expense involved in trying to (continuously) reinvent the wheel. Finally, in separating areas of the profession by skill and knowledge, we will benefit greatly from reference to the Cyber Security Body of Knowledge (CyBOK)[1] which has a wide range of material intended for use in the education and/or training of current or prospective practitioners.

[1] www.cybok.org
Accessed 2020 12 02

Career Frameworks and Specialisms

A career framework will need to use specialisms to demonstrate to an individual potential routes of a career from well defined starting points with particular skills and experience to achieving a flexible career incorporating the achievement of professional status. The framework should clearly show for a chosen specialism the qualifications, skills and experience required to achieve a particular level in the profession. It should clearly show the flexibility to both change specialisms and to utilise specialism in the later career stages to achieve senior management and executive roles. As career paths are inexorably linked to skills, behaviours and knowledge, a grouping based on skills and knowledge would seem to be the most logical approach.

Professional Register and Specialisms

A professional register will have to clearly show on what basis a person has been added so that it is clear what the underlying competences of a particular Register title is based upon. Specialisms in this case need to be linked to competency and skill to ensure transparency within the profession of what a particular person has been chartered against. Specialisms here need to adhere to a common competency framework but should be sufficient to differentiate between the actual competencies certified.

Existing Approaches

The NCSC has been investigating *Specialisms* as part of the review of the Certified Cyber Professional Scheme (CCP), and in 2018 identified two potential candidate areas; Risk Management and Security Architecture.[2] It is interesting that, whilst NCSC has been considering *specialisms* within the CCP scheme at a more defined level, in February 2020 the Government Security Profession launched its career pathway documentation.[3]

In the USA, the National Initiative for Cybersecurity Education (NICE) program initiated by the National Institute of Standards & Technology (NIST) developed a Cybersecurity workforce framework identifying seven speciality areas.

Globally, there are other lists of suggested *Specialisms*. Some the more relevant are discussed in more detail below.

Even if we cannot use the same approaches (there have been few attempts to develop one focused on career requirements through the entire spectrum of Cyber), these samples can provide usable input or partial approaches applicable to our requirements.

GSP

One of the concerns of the frameworks is a potential confusion of *specialisms* and *roles* or even *jobs*. The Government Security Profession (GSP) recognises this by stating:

> *The Government Security Profession Career Framework refers to roles rather than jobs. A role is an organised set of behaviours, responsibilities and activities granted to a person or team. One person or team may have multiple roles. Roles are about people, whereas jobs are about tasks and duties. Depending on the size of your organisation, you may carry out different aspects of multiple career framework roles on a day-to-day basis.*[4]

[2] https://www.ncsc.gov.uk/blog-post/setting-new-foundations-ccp-scheme?utm_source=IISP+Subscribers&utm_campaign=f81ceeb012-EMAIL_CAMPAIGN_2017_10_24_COPY_01&utm_medium=email&utm_term=0_32d07ba73f-f81ceeb012-107595495
Accessed 2020 10 03

[3] https://www.gov.uk/government/publications/the-government-security-profession-career-framework
Accessed 2020 07 23

[4] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/864753/Government_Security_Profession_career_framework_A_user_guide.PDF_pg15
Accessed 2020 07 20

The GSP[5] has defined four very high-level areas of security specialisation, along with an associated range of *Roles* (plus one additional category of *Corporate Enabler*). The 4 high level areas are:

- Cyber
  - Protecting information systems, the data on them and the services they provide, from unauthorised access, harm or misuse;
- Physical
  - Protecting physical assets, including people, services, infrastructure, systems, places, equipment and networks;
- Personnel
  - Mitigating the risk of our trusted people exploiting their legitimate access to an organisation's assets for unauthorised purposes;
- Technical
  - Holistically protecting sensitive information and technology from close access acquisition by hostile threat actors, as well as from any other form of technical manipulation.

The GSP approach is shown in Figure 1 (below).

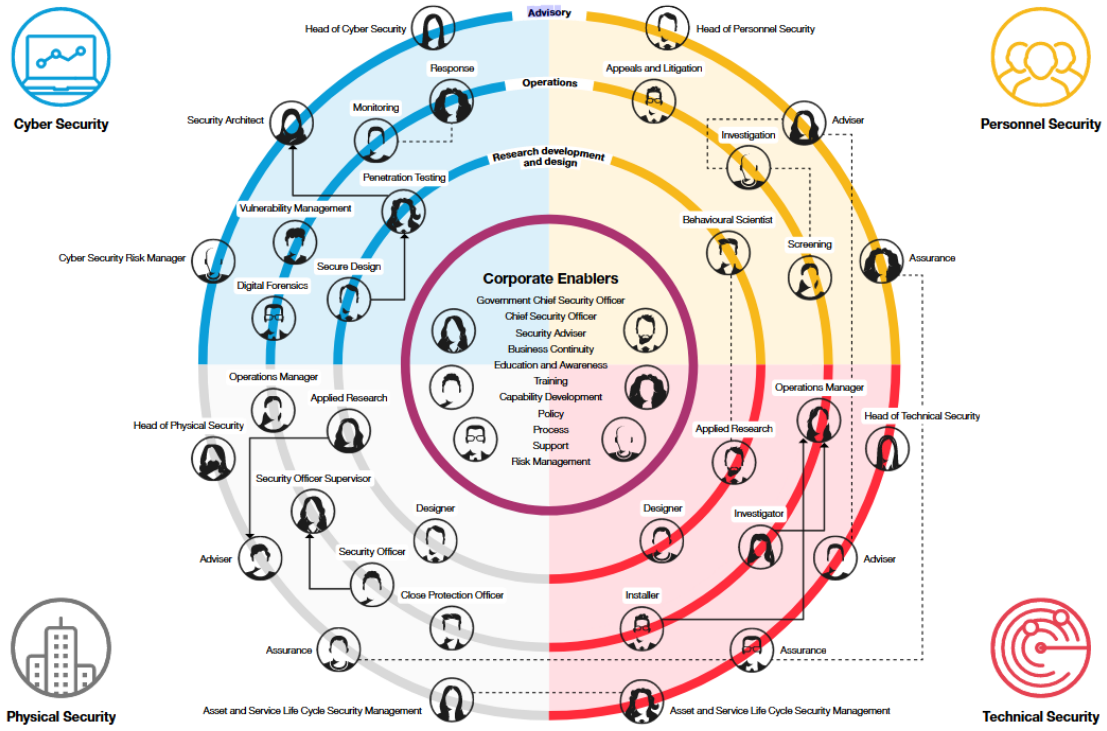


Figure 1: GSP Overview

[5] https://www.gov.uk/government/publications/the-government-security-profession-career-framework
Accessed 2020 09 21

NIST/NICE

In the USA, NIST established the NICE[6] initiative over a decade ago. NICE has also suggested a list of Speciality Areas[7]. The NICE National Security Cybersecurity Workforce Framework is described:

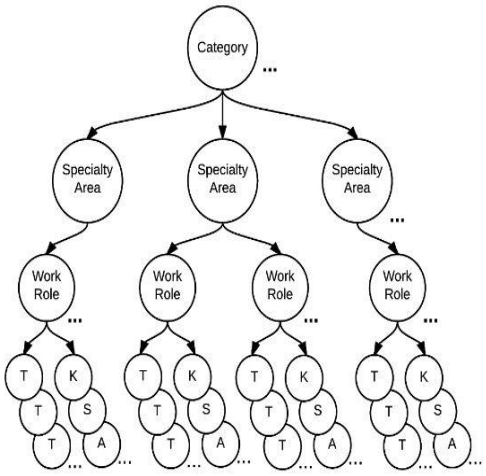
> *The Framework consists of thirty-one specialty areas organized into seven categories. These categories, serving as an overarching structure for the framework, group related specialty areas together. In essence, specialty areas in a given category are typically more similar to one another than to specialty areas in other categories. Within each specialty area, typical tasks and knowledges, skills, and abilities (KSAs) are provided.*[8]

NICE has defined a number of categories/areas of focus (based on security-related activities), shown in Figure 2 (below).[9]

Figure 2: NIST/NICE Areas of Focus

[6] https://www.nist.gov/itl/applied-cybersecurity/nice
Accessed 2020 09 21
[7] https://www.nist.gov/system/files/documents/2017/04/04/national_cybersecurity_workforce_framework_03_2013_version1_0_interactive.pdf
Accessed 2020 07 20
[8] https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=923472
Accessed 2020 10 02
[9] https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center
Accessed 2020 09 21

In support of each of seven identified categories/areas of focus, NICE has established a simple flow, shown Figure 3.[10] The current state of the NIST/NICE exercise is a published package which covers:



- seven Categories (our 'High Level *Disciplines*')
- 31 Specialty Areas (our 'Disciplines')
- 52 Work Roles (our 'Specialisms')
- ~1,000 Tasks (our 'Specialisms and *Skills*')
- covered by ~1,180 KSAs (largely agreeing with the content of CyBOK).

Figure 3: NIST/NICE Flow

As expected, other agencies in the USA are supporting the NICE framework. For example, the Cybersecurity and Infrastructure Security Agency (CISA) has recently released an interactive application which users can use to chart a career path based on the NICE content.[11]

GIAC

In contrast to the two high-level approaches above, there are also much more focused approaches which cover specific areas of cyber security, but these do not try to cover all the specialist areas of cyber security. One such is Global Information Assurance Certification (GIAC) which states:[12]

> *The primary goal of the program is to address the need to validate the skills of security professionals and developers. GIAC certification provides assurance that a certified individual meets a minimum level of ability and possesses the skills necessary to do the job. The standards for the GIAC certification were developed using the highest benchmarks in the industry.*

This again confuses the *specialism* with the training and the *skills* required for the *role*, which for the purposes of the UK CSC and the cyber practitioners we need to separate clearly.

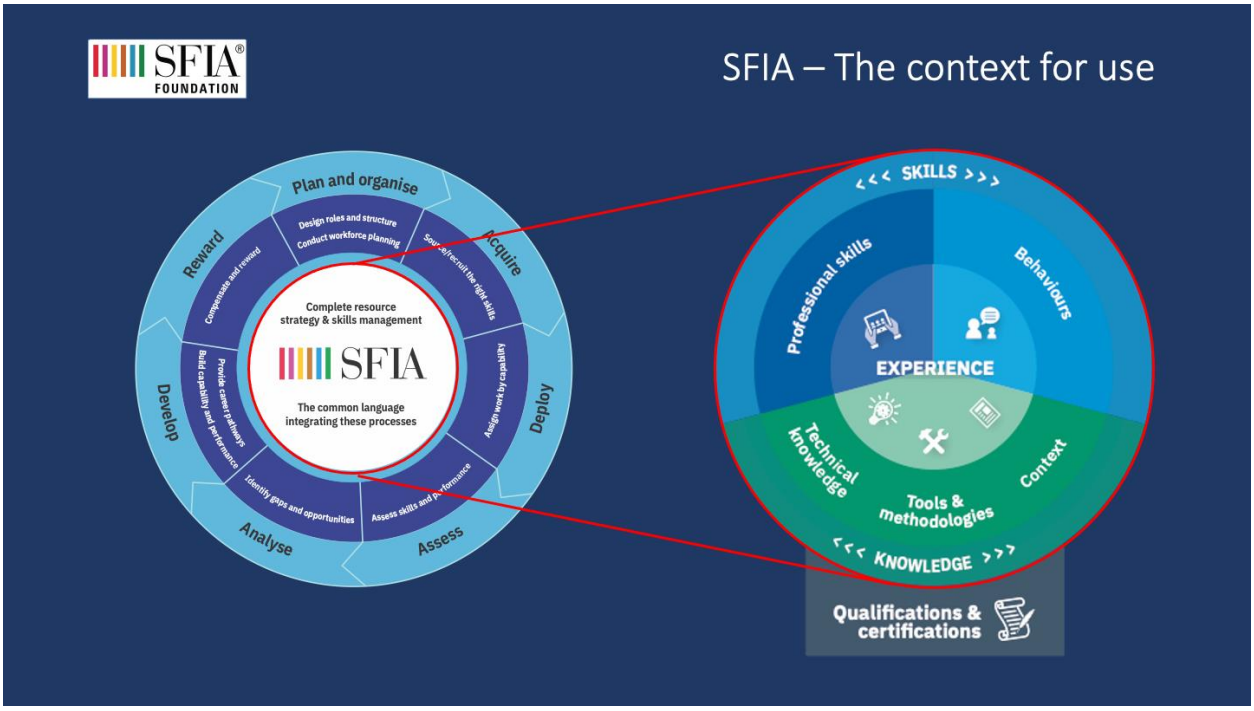
[10] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf
Accessed 2020 09 21

[11] https://federalnewsnetwork.com/workforce/2020/09/cisa-wants-to-help-cyber-professionals-map-out-a-career-path/
Accessed 2020 09 22

[12] https://www.giac.org/about/mission
Accessed 2020 09 21

SFIA

SFIA is a skills and competency framework covering the breadth of IT, Digital Transformation and Software Engineering. Originally developed for the UK (by a collaboration of UK companies), SFIA now has a global footprint and is used by individuals, corporates, professional bodies and governments in over 180 countries. It continues to be developed by open-consultation but this has, for around 15 years, been a global effort.



SFIA is a 7 level framework of Levels of Responsibility, characterised by a number of Generic Attributes (5) which characterise behaviours and 102 Professional Skills. SFIA recognises the importance of Knowledge and the place for certifications and qualifications. But most importantly Experience is at its core – you have a skill at a particular level because you have demonstrated evidence that you have practiced that skill at that level.

SFIA is used in many different ways. One common way is to plan and organise a workforce – an organisational design. In a similar manner SFIA is used by professional bodies for the evaluation of individuals for the equivalent of 'Chartered' or 'Technician' (BCS, IET, ACS, ITPNZ, CIPS and IITPSA use SFIA Level 7 for their CIO Accreditation, IFIP/IP3 use SFIA as their 'Gold Standard' for professional certifications for professional bodies). This leads to 'equivalence' internationally, for instance BCS CITP aligns as ACS Certified Professional; BCS RITTECH aligns with ACS Technologist.

SFIA has since 2000 had security skills within it, over successive versions the skills have been refined and refreshed to SFIA 7 (2018) where there are currently 5 explicit security skills, and

security is a part of 20 other professional skills and also explicit as part of the Generic Attributes. There is current work going on to update SFIA for release as SFIA 8 in 2021 and a number of working groups are helping with this. Once again a review with regards to information/cyber security is underway along with many other themes (AI/ML/DS for instance).

The Information security working group has so far mapped SFIA to NIST/NICE areas and is working to identify necessary actions for the SFIA 8 refresh including updates to skills and the further development of an information/cyber security view of SFIA a key element of which is likely to be both a recognition of skills appropriate to a specialism, that specialists need non-specialism skills and also the position that security is part of everyone's role.

CIISec Skills Framework

Another Skills framework that is more focused on Information Security is that of the Chartered Institute of Information Security (CIISec).

The CIISec Skills Framework first published in 2006 was developed to describe the range of competencies expected of Information Security and Information Assurance Professionals in the effective performance of their roles. It was developed through collaboration between both private and public sector organisations and world-renowned academics and security leaders. The Framework defines the skills and capability expected of security professionals in practical application and is not just an assessment of their knowledge. Version 2 issued in 2015 was the result of an extensive review to recognise that the profession had evolved significantly and reflects new Cyber Skill profiles and was the result of an extensive consultation exercise with a wide range of public and private stakeholders. Since then the Framework is reviewed annually on this basis to ensure that it captures changes in the profession and evolving skills areas.

It has Eleven security disciplines areas, labelled from A-K, as shown in the diagram below to cover the range expertise across the profession. These are supported by approximately 30 skills areas. Sections A-I describe the breadth of technical or specialist skills areas that can be covered by information and security professionals; section J describes the interpersonal and business skills expected of professionals and section K the professional commitment to and development of the profession. Version 2 has six skills levels to measure capability and competence level, ranging from knowledge and understanding with little or no practical experience (levels 1 and 2), to a standard practitioner level with some practical experience (levels 3 and 4), to being able to apply the skills area with a high level of competency at a senior practitioner with autonomy and with very little oversight from others (levels 5 and 6).

The CIISec Skills Framework is the standard on which CIISec members are assessed and accredited. Within CIISec the Framework is also used to accredit commercial training courses and certifications, assess eligibility of universities for its academic programme and to shape its professional development programmes.

Within Government, it underpins many of the areas defined in the recently issued UK GSP model discussed above and is used similarly by the ACSC in Australia.

The Framework underpins the National Occupation Standards (NOS) for Cybersecurity which is the foundation standard for the development of under-graduate programmes, apprenticeship programmes. Commercial Training organisations are also using the CIISec Skills Framework to develop and align course content.

Commercial and public sector organisations use the CIISec Skills Framework in their employee career development programmes to define the skills and capabilities expected of their security professionals. It is an integral part of the CIISec Capability Development Methodology (CDM) which assists organisations to recruit, develop, deploy and maintain security skills. The CDM uses the Skills Framework in conjunction with the CIISec Knowledge and Roles Frameworks to achieve this.

As with SFIA the skills areas have been mapped to the NIST and NICE and also to the College of Policing Skills Standard for the Cyber Digital Investigation Profession.

IT National Occupational Standards

National Occupational Standards (NOS) specify UK standards of performance that people are expected to achieve in their work, and the skills and knowledge they need to perform effectively. The standards are used in Northern Ireland, Scotland and Wales to directly inform and support vocational qualifications, apprenticeship development and national training

programmes. There are 9 completed standards in IT Cyber Security[13] and another 86 in Information Security (IT and Telecoms Professional).

Cyber Security is subdivided into a number of sub-areas and then standards developed against those areas to demonstrate competence.[14]

The sub areas identified are split into two groups Cyber Security and Cyber Resilience the former being attached to IT Professionals and the latter to the wider workforce.

Developing a hierarchical model which could operate for the UK CSC

Why a hierarchical model?

It is recognised that a cyber career is varied and that there are multiple entry points, so any system adopted to classify skills and knowledge needs to be flexible to ensure that it can be recognised from the classification what an individual is skilled at and can offer the profession as well as allow the individual to navigate a career path that is as flexible as possible with clear decision points on the acquisition of both skills and knowledge.

It is also important that a methodology is developed so that the council can govern specialisms to ensure consistency and transparency as licensed bodies across the spectrum of the profession provide new routes to charter.

There are levels of decomposition that allow for an individual to seek or a Professional Body to give appropriate direction and guidance. It is however important to realise that individuals are likely to engage with the profession either through a professional body appropriate to their skills utilising the careers framework to inform their choice.

The proposed hierarchy is made up of 3 levels – see Figure 8 (below). In the future the council may choose to concentrate at the specialism level only as the main purpose of High Level Disciplines and Disciplines is to signpost from existing bodies with established disciplines to the cyber security specialisms.

	Name	Definition and use
1	High Level Discipline	The areas of focus of the UK CSC. These are used to help someone trying to join the profession to choose the most appropriate Professional Body

[13] www.ukstandards.org.uk
Accessed 25 10 20

[14] https://odag.co.uk/wp-content/uploads/2020/08/IT-National-Ocupational-Standards-Overview-Booklet-July-2020-ODAG-Consultants-Ltd.-1.pdf
Accessed 25 10 20

2	Discipline	The *disciplines* as defined by the Professional Body dividing up the range of areas in which they offer help, guidance and training to the new and existing members of the profession
3	Specialism	The subsets of areas of focus within a *Discipline* separated by skills and knowledge. It is at this level that training is likely to take place. Specialisms are likely to exist within multiple disciplines dependent on the High Level Discipline of a particular professional body
4	Role	The job a person does. To do the role they will require *specialisms* and *skills* at a competency level as set out in a particular job specification.

Figure 4: Simplified Hierarchy

In this hierarchy, we believe that the qualification given at a registered level should not be subdivided. The Specialism in which the individual is most proficient should be specified according to the disciplines of the Professional Body.

In all cases, *Disciplines and Specialisms* should be capable of being validated by the appropriate Professional Body against both the Professional Standard and the skills, competency and knowledge required by the professional body to achieve a particular professional status.

High Level Disciplines

Staying with the two high-level models (GSP & NIST/NICE) we look at their *High-Level Disciplines* and compare those to the preliminary list from the UK CSC shown in Figure 5 (below).

NIST/NICE	GSP	UK CSC
Analyze	Cyber Security	Analysts & Programmers
Securely Provision	Physical Security	Auditors
Operate & Maintain	Personnel Security	Engineering
Oversee & Govern	Technical Security	Forensics & Investigations
Collect & Operate	Corporate Enabler	Information Security
Protect & Defend		
Investigate		

Figure 5: High Level Disciplines

As the three sets of *High-Level Disciplines* are derived from differing approaches it is very evident that there is no easy correlation. The advantage to the UK CSC of using its own set of *High-level Disciplines* is that these could be used by the bodies who will be actively participating in the Council to define the relevant *Disciplines* for evaluation for Charter purposes and to link to skills and roles.

We would caution against allocating the High-Level Discipline to a Chartered status – better to leave the skillset to the disciplines and specialisms shown by the individual's CV. This approach has been used very successfully in, for instance, the accountancy profession where the

qualification of ACA (later FCA with experience) is not differentiated by the discipline or specialism of company taxation, personal taxation, audit, insolvency, risk or management accounting as examples.

A (very) preliminary list linking *Professional Bodies* to *High Level Disciplines* is shown in Figure 6 (below).

UK CSC Discipline	Professional Body
Analysts & Programmers	IAP, BCS
Auditors	IIA, ISACA
Engineering	IET, InstMC
Forensics & Investigators	CSFS, CREST
Information Security	CIISec, ISACA, $(ISC)^2$

Figure 6: UK CSC Disciplines to Professional Bodies

Having these *High-Level Disciplines* would be of extreme value to the potential entrant. If you have a person who has taken a degree in Computer Science, for example, but wishes to move into cyber security, they are more likely to find their path through the BCS or IAP, which narrows their search in this complex environment. This does not mean that the BCS or IAP is not in the other areas, it merely shows their primary focus. Similarly, a person taking forensics who wishes to qualify in cyber security would likely look to CSFS or CREST in the first instance.

Disciplines

Following agreement as to the high-level areas of focus, each Professional Body would then be able to address the *Disciplines* which define the *High-Level Discipline*. This would be based on their Royal Charter and their declared areas of concentration. This approach also shows that as new fields arise and new organisations come into being, they can follow this approach and be added to the UK CSC High Level Disciplines without having to redo the whole structure to accommodate.

As an example: Using Information Security as the *High-Level Discipline* and the CIISec as the Professional Body, CIISec uses its Skills Framework to identify 11 *Disciplines* made up of a blend of technical and soft skills:

- Information Security Governance & Management;
- Threat Assessment & Information Risk Management;
- Implementing Secure Systems;
- Assurance: Audit, Compliance & Testing;
- Operational Security Management;
- Incident Management, Investigation and Digital Forensics;
- Data Protection, Privacy & Identity Management;
- Business Resilience;

- Information Security Research;
- Management, Leadership, Business & Communications.

These 11 *Disciplines* are then further subdivided into *Specialisms* to cover specific areas such as risk management, incident management, privacy and data protection. The high-level mapping between the UK CSC and NICE can then be shown as in Figure 7 (below). This could be repeated for GSP.

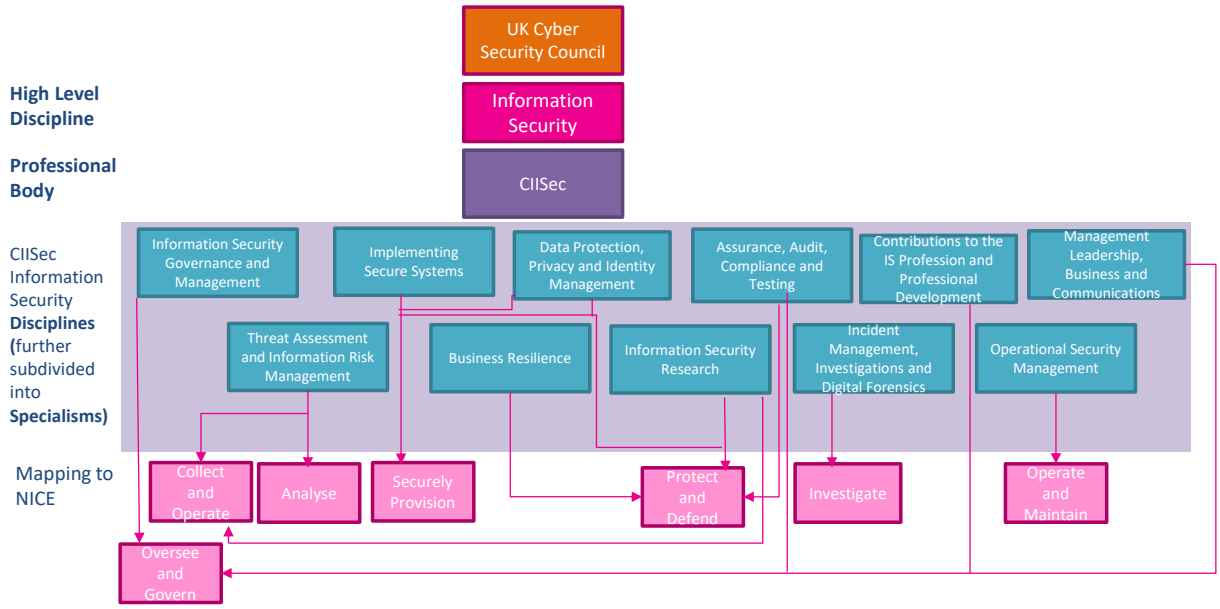


Figure 7: Sample Mapping of Specialisms to UK CSC & NICE (similarly this can be completed for GSP)

Specialisms

A *specialism* then becomes a subset of a discipline. Following the CIISec example above, taking Information Security Governance and Management, this can be further subdivided by *Specialism* into:

- Governance
- Policy and Standards
- Information Security Strategy
- Innovation and Business Improvement
- Behavioural change
- Legal and Regulatory Environment and Compliance
- Third Party Management

Skills

A constituent part of *Specialisms* are *the* underlying skills. Many skills are required across a range of disciplines – these are such as aural, presentation and writing skills, people management, project management, spreadsheet development to name a few common ones.

Some *skills* can be enhanced by training for *Certification*, whilst others are best learned on the job, or by following others' example. It is acknowledged that skills may wax and wane as the practitioner's role or specialism changes.

Also, it is important to keep in mind the skills a practitioner requires as (for example) the Head of Third-Party Security are different from those as a practitioner in that sector. To complete a third party review, the ability to question and listen to the third party, analyse the information collected and summarise the key issues found is invaluable. The Head is likely to be called upon to act more at the strategic level, is probably responsible for the questions the team asks as well as the details within the third party contracts; the Head must be a good people manager. It is also important to recognise that the level of competency in a particular specialism may change dependent on the role.

Roles

A *Role* is the function an individual performs. This will vary by industry sector and by the needs of the organisation. In some organisations, cyber security will be part of a single person's *role*, while in others there can be many hundreds of people performing cyber security tasks. There can also be differentiation by skill level, for example: Apprentice, Junior Practitioner or Senior Practitioner.

Certifications/Qualifications

Some roles may require *Certifications.*[15] Other roles may have preferred *Certifications* to ensure a base level of knowledge. In either case, a *certification* normally involves some combination of study plus experience, verified through a formal examination of some form. The training associated with a certification is usually highly focused and task-specific, but seldom needs to be renewed[16]. Continuous professional development becomes mandatory in the fast-moving technology led environment. Some Certifications will be linked to Specialisms, but many will cover multiple specialisms or be role specific.

[15] Refer to the work of Paul Jerimy for an example of the certification classification schemes available https://pauljerimy.com/
Accessed 2020 09 23

[16] An exception is the PCI DSS qualifications of ISA and QSA where the training and certification is renewed annually. See https://www.pcisecuritystandards.org/program_training_and_qualification/qsa_certification Accessed 2020 10 04

Conclusion / Way Forward

Initial Set-up and Governance Structure

This paper gives an outline of a framework to begin to classify the profession so that we can clearly articulate the areas of competence that cyber security covers. It is envisaged that the initial disciplines will be taken-up by the Professional Bodies and the specialisms defined under those bodies to allow a Chartered Status and other titlesof registration to be identified by the designated specialism. This allocation of Specialisms will need to be governed by the Council to ensure consistency and a common lexicon between the licensed bodies to create a clear register of professionals.

In addition, specialisms as a grouping of roles will allow a consistent approach to career frameworks, demonstrating to aspiring professionals the routes to a career in Cyber to Chartered Status but eventually to Senior and Executive Roles as leading Professionals. The use of specialisms will be an interim measure until Standard Occupational Classifications are further defined for Cyber Security but will highlight the flexibility of careers and the decision points and implications of following a particular specialism.

A managed maintenance programme will have to be established to ensure the UK CSC is able to maintain an 'evergreen' approach to the *Skills* [competences] and *Specialisms* required by the individual practitioners. This programme would be under the governance of the appropriate committee.

It is envisaged that registering more specialisms would be via a constructive challenge process, with some public consultation with the community organised by the sponsoring body and a final recommendation and decision by the Council. Community consensus should ensure that the specialisms are applicable and relevant to the needs of the profession.

As the entire cyber field develops and expands, the need to focus on ever more concentrated areas will continue. The Professional Bodies already monitor their *Disciplines, Specialisms* and *Skills [as before]*, and that, through the linkage between the Professional Bodies and the UK CSC should ensure that the UK CSC can maintain its flagship status as the body for the cyber security professional within the UK.

How does this work for individuals?

This Specialism paper provides a framework that should allow the variety of Cyber Security careers to be communicated by the council and its licensed bodies. It allows for clear career

frameworks to be established for specialisms and hence communicating the skills and qualifications required not only to enter the profession but also at key points in early and mid-career the opportunity to progress within a specialism or indeed change direction. It also clearly identifies the area of cyber security that an individual is competent in by the area of expertise on the professional register to communicate to prospective employers and clients.

UK CSC Specialisms

The framework defines the process on how a professional body can define specialisms under the governance of the council, but there is a need for an initial set of Specialisms. These Specialisms need to be defined by disparate skills and link to real world roles via the careers framework and professional register. It is therefore recommended that the initial list of cyber specialisms instigated by the council are based upon a consolidated list from existing frameworks. The reasoning behind this is that the existing frameworks have matured over a number of years and are used widely to help define cyber based roles within organisations. The frameworks used to consolidate a list were:

- The National Occupational Standards for Cyber Security and IT security (NOS)
- The CIISec Skills Framework
- The CIISec Roles Framework
- The Government Security Profession Careers Framework (GSP), including related, equivalent private sector roles
- The Australian Public Service Digital Careers Pathways including the prototype Career Pathfinder (APS Pathways)
- Skills for the Information Age (SFIA)
- The 15 roles identified in the CompTIA Report for Skills Development Scotland
- The National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NICE Framework)
- NICE CyberSeek Career Pathway Tool (CyberSeek)
- Australian Signals Directorate Cyber Skills Framework (ASD Framework)

This does NOT preclude a professional body defining appropriate specialisms under their ascribed cyber disciplines.

1. **Cyber Security Policy and Management**-Directing, overseeing, designing, implementing or operating policies and procedures at an enterprise level in line with business objectives and regulatory requirements.

2. **Risk Assessment and Management**- Directing, managing, maintaining and applying plans, controls and processes to identify and evaluate cyber security risks, and to propose and monitor countermeasures to these, in line with an organisation's policies and risk appetite.

3. **Secure System Architecture Design** – Designing the technical controls to meet the security requirements of a system (IT, IoT, Industrial control, network) etc., balancing with the functional requirements of the system.

4. **Secure System Development** – Implementing a secure system, product or design to meet either the architectural or technical security requirements, throughout the lifecycle of the system, product or design.

5. **Security Testing**- Testing a system, product or design, against the specified security requirements and/or for vulnerabilities that could be exploited by an attacker whilst a system is deployed.

6. **Data Protection and Privacy Management**- Managing the protection of personal data at an enterprise level, enabling an organisation to meet the legal and regulatory requirements.

7. **Audit and Assurance**- Verifying that systems and processes meet the specified security requirements and that processes to verify on-going compliance are in place.

8. **Threat Intelligence**- Assessing and validating information on current and potential cyber threats to maintain an organisation's situational awareness.

9. **Vulnerability Management**- Managing the configuration of protected systems to ensure that any vulnerabilities are understood and managed in accordance with an organisation's security requirements, risk appetite and threat intelligence.

10. **Secure Operations**- Ensuring that an organisation's operations of it information systems are in accordance with the agreed Security Policy. This includes establishing secure operating procedures and maintaining the configuration of supporting technical devices including firewalls and protective monitoring tools

11. **Identity and Access Management**- Directing, overseeing, designing, operating and applying policies, procedures and controls to ensure that access to information or computer-controlled resources is only for authorised use by authenticated individuals.

12. **Network Monitoring and Intrusion Detection**- Monitoring network and system activity to identify unauthorised actions by users or potential intrusion by an attacker, and analysing information to initiate an organisational response to the potential breach.

13. **Incident Response**- preparing for, handling and following up cyber security incidents, to minimise the damage to an organisation and prevent recurrence.

14. **Digital Forensics**- deeply analysing a security event in the aftermath of a breach and in the case of legal action capturing evidence in line with legal requirements so that evidence may be presented in court.

15. **Cryptography and Communications Security**- Designing, developing, implementing and testing a system or product to provide cryptographic and/or secure communications to meet an organisation's security requirements and appropriate regulatory standards.

As an example, if we were to break down a Specialism above say Cyber Security Policy and Management it would cover skills such as Governance, Policy and Standards, Information and Security Strategy, Innovation and Business Improvement, Human Factors and Behavioral Change. It would cover roles such as CISO (Chief Information and Security Officer) and CTO (Chief Technology Officer).

It also envisaged that specialisms would cover all application where cyber security skills are demanded including Internet of Things, Industrial Control, Industry 4.0 and traditional network and IT Systems.

Sample Career Pathways

Penetration Testing

Using a Penetration (Pen) Tester as an example of how all of these fit together to form a career pathway, the *Specialism* Security Testing includes a variety of Penetration Testing Roles:

- Internal Network Tester: an employee focused on network vulnerabilities, primarily from an internal viewpoint;
- Ethical Hacker: an external contractor likely engaging the network from the outside;
- Bounty Hunter: a freelancer who finds vulnerabilities in software and sells the knowledge to a vulnerability broker or directly to the software manufacturer.

The common thread across these roles is the specialism. This means that a new entrant to cyber could go to the careers framework and identify the skills and certifications required to match an entry level role. The same entrant could then trace a path through the framework to more experienced and senior roles understanding the skills developments and certifications required at each level.

The aspiring professional could also look at other specialisms and understand how the skills gained as a tester could be applied to other roles allowing for changes of direction e.g. Incident Responder or Senior SoC Analyst.

A Professional Body could decide to offer a Chartership based on Pen Testing. Based on the pathway developed through the lower tiers, the candidate practitioner would be able to focus efforts on the Professional Body that seems to be best aligned with their aspirations. In our example of a Pen Tester,

- If the person wishes to become an ethical hacker CREST may well be the first choice,
- An IT person who moves into internal pen testing may look at the BCS, and
- A person with both good technical and contract skills may be attracted to be Head of Pen testing and choose CIISec.

However, this may vary dependent on the career aspirations of the individual. The key is that specialisms are tied to skillsets in a structured way so that it is transparent what the Chartership applies to.

Audit

Auditor is another widely used term for a variety of *Roles* which fit under the *specialism* of Audit and Assurance. Auditors in the cyber world focus on technology and essential Governance, Risk & Compliance issues. In the 3 line Model Auditors are independent and responsible for checking the first two lines (Risk Management and Assurance).In some organisations, the roles of Assurance and Audit are combined, but the key is that this person does not do the controls (the 1st line function), rather they check that the control or function is being operated correctly or effectively. As with the Pen Tester, the *Specialisms and skills* (and associated *Certifications*) would be roughly the same across the board for the various types of Auditor but the differences lie in how the *Skills* are used and to what end (the *Role*).

Based on the ISACA framework, some of the easily identifiable audit *Roles* (and the associated *Certifications*)[17] related to cyber include:

- Auditor involved in the audit, control, monitoring and assessments of an organization's information technology and business systems: Information Systems Audit (CISA);

[17] All cited drawn from Wikipedia entry for ISACA at: https://en.wikipedia.org/wiki/ISACA
Accessed 2020 10 02

- Auditor utilizing expertise in identifying and managing enterprise IT risk and implementing and maintaining information systems controls: Risk & Information Systems Control (CRISC);
- Auditor directing, managing and supporting the governance of IT: Governance of Enterprise IT (CGEIT).

Again, the common thread is that all these *Roles* use approximately the same set of *Specialisms*, but at different levels of expertise.

It is important to remember that while Audit is clearly identified as a *Discipline* in the UK CSC scheme, it may also exist as a *Specialism* under one of the other *Disciplines*.

Based on the pathway developed through the lower tiers, the candidate practitioner would be able to focus efforts on the Professional Body that seems to be best aligned with their aspirations. In the example of Audit, ISACA may well be the first obvious choice. However, there are several other professional designations which may be acquired elsewhere (IIA as an example) and applied successfully within cyber.

Further work

The Council should work with ONS (Office of National Statistics) to define further Standard Occupational Classifications for Cyber aligned to specialisms. This would improve visibility of cyber roles through the wider community and facilitate a common lexicon in the future across the licensed bodies.

The Council should look at future alignment with SFIA the leading global framework establishing a line of influence, this again would facilitate a common lexicon and more transparency across the technical bodies. This should not discourage bodies having their own frameworks to meet their membership needs but again these could align to a global competency framework such as SFIA.

With a completed and agreed-upon hierarchy, the Professional Bodies can establish a flow both within their *Disciplines* & *Specialisms* and the supporting *Certifications* which can then be used as a clear reference and guide for cyber practitioners. This should then satisfy the requirements of the UK CSC and be flexible enough to cope with the ever-changing scope and boundaries of the profession of cyber security.