UK CYBER SECURITY COUNCIL PROPOSAL FOR THE

UK CYBER SECURITY COUNCIL STANDARD FOR PROFESSIONAL COMPETENCE & COMMITMENT (UK CSC SPCC)

Version 1

VERSION CONTROL

Date	Version Number and File Reference	Changes	By
19th January 2021	Issue v0a	Removed from working document to stand alone standard document.	RI
22nd January 2021	Issue 1	Final document for Community Challenge	RI, ND, SP, BR

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

The UK Cyber Security Council (the Council) would like to acknowledge the assistance and support of the Engineering Council in the preparation and delivery of the Cyber Security Council Standard for Professional Competence and Commitment (UKCSC SPCC). To establish a new National Standard for Professional Competence and Commitment in such a short time could not be achieved without taking account of the good and established practice from a similar Council body and we are grateful to the Engineering Council not only for their advice and support but their willingness to allow the Council to utilise their UK-SPEC framework as the basis for the UKCSC Standard for Professional Competence & Commitment.

We wish to extend our thanks to those Cyber Security Alliance organisations who provided access to their own routes to Professional Registration and the standards that are applied, namely:

- BCS The Chartered Institute for IT (BCS)
- The Institute of Engineering & Technology (IET)
- The Chartered Institute for Information Security (CIISec)
- The Chartered Society of Forensic Sciences (CSFS)
- The Ministry of Defence (MoD)
- The Royal Institute of Chartered Surveyors (RICS)
- The Royal Pharmaceutical Society (RPS)
- The Royal Society of Chemistry (RSC)
- The Chartered College of Teaching (CCT)

We wish to extend our thanks to those individuals who responded to the UK CSC SPCC survey, namely:

- Ollie Whitehouse – NCC Group
- Dr David King – Legal & General
- Peter Hazel – Yorkshire Water
- Ben Franklin – BSIT
- Member – MoD Cyber Legal Team
- Mark Lees – DVLA
- Member – Cabinet Office Security Profession Team
- Nicholas Cooper – Health Care Professional

BACKGROUND TO THE STANDARD DEVELOPMENT

Developing a standard for Cyber Security Professionals brings together a number of documents developed during the Council formation project and includes:

- CPD
- Discipline / Specialism
- Registration Titles
- Licensing
- The Professional Register
- Benefits
- Individual Application Process for Professional Registration
- Cyber Security Qualifications Framework
- Code of Ethics Guiding Principles – Individual
- Code of Ethics
- Ethics Case Studies

These documents provide the detail related to a particular element of the professional registration standard, the processes applicable to professional registration and the requirements of the licensed organisations that will be responsible for assessing individuals. This left the actual requirements for Competence & Commitment that are required for a individual to be assessed against when applying for professional registration.

A twin-track approach was taken in the development of the detailed requirements of the standard. This was to ensure that the uniqueness of cyber security was identified, recognised and understood and further, to ensure that anyone who qualifies for professional registration meets all the requirements of someone working within the Cyber Security Industry. The first of the two tracks reviewed existing routes to chartered status, to confirm understanding and identify best practice which could then be utilised as appropriate. The second track was a small survey of individuals who hold senior cyber security roles and responsibilities in order to understand the requirements from a practitioner and industry perspective.

The analysis of existing routes to chartered status looked at both Cyber Security Alliance organisations and other organisations outside of the Alliance in order to provide a broad and comprehensive understanding of the chartered status requirements for the analysis.

A key aspect of this analysis was to differentiate between professional registration with the Council and membership of a professional membership organisation. Whilst registration with the Council will require that individuals are members of a professional membership organisation, the grade of membership is not stipulated by the council. Any mapping of membership organisations' grades of membership to the professional registration titles is purely a function of the membership organisation.

Combining the best practice with both the analysis of existing routes to professional registration and the survey of senior cyber security professional feedback, provided the content for the development of the Cyber Security Professional.

THE UK CYBER SECURITY COUNCIL STANDARD FOR PROFESSIONAL COMPETENCE & COMMITMENT

THE COUNCIL REGULATIONS & STANDARDS

The UKCSC SPCC is not contained in a single document. It is a collection of documents that, together, cover the various elements of the standard in more detail and, when linked to the Council formation documents, comprise the overall Council regulations. The diagram at Figure 1 depicts the documents that relate to professional registration, the professional registration standard and the overall relationship between them.

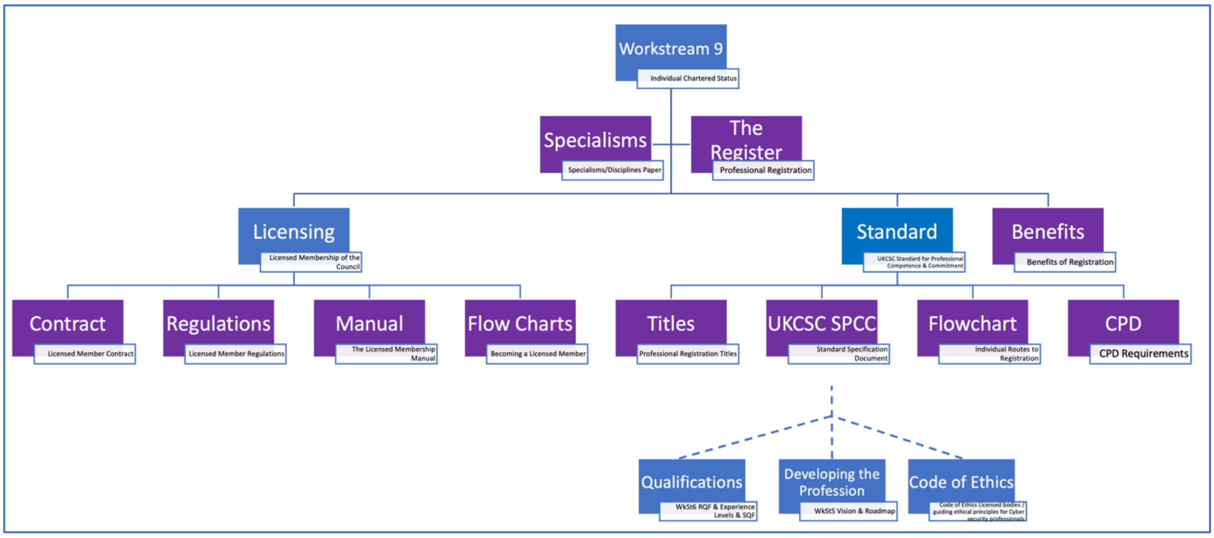
Workstream 9
Individual Chartered Status
Specialisms
Specialisms/Disciplines Paper
The Register
Professional Registration
Licensing
Licensed Membership of the Council
Standard
UKCSC Standard for Professional Competence & Commitment
Benefits
Benefits of Registration
Contract
Licensed Member Contract
Regulations
Licensed Member Regulations
Manual
The Licensed Membership Manual
Flow Charts
Becoming a Licensed Member
Titles
Professional Registration Titles
UKCSC SPCC
Standard Specification Document
Flowchart
Individual Routes to Registration
CPD
CPD Requirements
Qualifications
WkSt6 RQF & Experience Levels & SQF
Developing the Profession
WkSt5 Vision & Roadmap
Code of Ethics
Code of Ethics Licensed bodies / guiding ethical principles for Cyber security professionals

Figure 1 - The Council Professional Registration Document Relationship

THE PURPOSE OF THE COUNCIL STANDARD FOR PROFESSIONAL COMPETENCE AND COMMITMENT

The scope of the Council is focused on the themes of; Professional Development, Professional Ethics, Thought Leadership and Influence and Outreach and Diversity, (UKCSC), (DCMS, 2018).

Professional Development
Outreach and Diversity - Developing the Next Generation
UK Cyber Security Council
Professional Ethics
Thought Leadership and Influence

Figure 2 - The Council Four Themes

The Cyber Security Council Standard for Professional Competence and Commitment must, therefore, include these themes as they apply to individuals working in the profession and, in turn, how those individuals apply these attributes as they carry out their roles and responsibilities.

Professional Development – relates to the individual as well as the Council and each registered professional is required to demonstrate their commitment to professional development within their Discipline / Specialism as well as how they mentor others on their journey to become professionally registered.

Professional Ethics – is an attribute that must be upheld and whilst the council can set the standards it is up to the individuals who are professionally registered to ensure that their day-to-day actions are of the highest ethical and moral standard.

Thought Leadership and Influence – a Registered Cyber Security Professional is a senior leader within the cyber security industry and is required to constantly maintain and improve their knowledge and experience as advances in cyber and cyber security occur. As a professional they are also charged with mentoring and influencing those immediately in their charge along with the wider industry as opportunities allow.

Outreach & Diversity, Developing the Next Generation – A significant aspect of being a Cyber Security Professional is a commitment to recognise opportunities to be inclusive and diverse within their day-to-day roles and responsibilities. This commitment goes beyond day-to-day activities; a registered professional should be expected to look for, create and develop the next generation of cyber security professionals.

PROFESSIONAL REGISTRATION

The objectives of the Council are:

"To promote high standards of practice in the cyber security profession for the benefit of the public. In particular, but not exclusively, by advancing education in the subject of cyber security and through the development, promotion and stewardship of nationally recognised standards for the cyber security profession."

In pursuance of the objectives, the Council will:

1. Maintain a register for Cyber Security Practitioners, with sections for each Professional Registration Title.

2. Establish and keep under review:

    - Generic standards and procedures for academic and/or vocational achievement, professional competence, and commitment.
    - The requirements for initial and continuing professional development for Registrants (see Continuing Professional Development CPD).

3. Provide guidance on the codes of ethics and conduct and disciplinary procedures for Registrants which will be applied through the Licensed Bodies for example, through inclusion in their own codes and procedures.

4. Licensed Bodies that have met the relevant requirements to assess and recommend individuals that are their members for admittance to the Register under the titles that they are licensed to assess.

5. Designate as Registrants those Individuals assessed as meeting the relevant criteria as provided by the Council.

6. Take any action it deems necessary to protect the integrity of the Registers and to ensure that its post-nominal designations are used only by those Registrants entitled to do so.

7. Have an appeal process for individuals who have been assessed as not (yet) meeting the standards of competence.

PROFESSIONAL REGISTRATION TITLES

Three titles of professional registration are defined:

a. Chartered
b. Principal
c. Associate

The number of professional registration titles is a function of the Council recognising the breadth and depth of roles and expertise within the cyber security sector. Having more than one title enables individuals to attain a certain level of competence and commitment, and then either to stay with that title or to chart a route to Chartered professional registration should they wish to do so.

Licensed Bodies may link the Council Professional Registration Titles (and other professional qualifications) to their organisation membership grades. The Council professional register is not associated with any organisational membership grades. The individual Licensed Bodies will decide if they want to map the professional registration titles to their own individual organisational membership levels.

DEMONSTRATION OF SPECIALISM

The Council will maintain one Register with specialisms effectively implied by the licensed body through which the individual has aligned themselves and chosen to apply (i.e., the Licensed Body). There will be no identification of specialisms within the professional titles.

The detail on specialisms (and disciplines) can be found in the supporting Discipline / Specialism document.

POST NOMINALS

Post nominals are used as recognition and as a 'badge of honour.' The proposed Council professional registration post nominals are:

a. CCySyP – Chartered Cyber Security Professional
b. PCySyP – Principal Cyber Security Professional

c. ACySyP – Associate Cyber Security Professional

BENEFITS OF REGISTRATION

INTRODUCTION

Society necessarily places great faith in its cyber security specialists. In our modern, digital world, we expect them to keep us secure from threats, vulnerabilities, attackers, thieves, and criminals. We expect them to ensure that we can, as individuals, safely read the news or do our personal banking on our mobile devices and simultaneously expect them to protect critical national infrastructure from attacks by malevolent actors.

The UK Council register is the only complete UK register of professional cyber security professionals. All individuals on the register, regardless of the title under which they are registered, will be professionals who have met the UK Cyber Security Council Standard, meaning they have:

- achieved the required level of experience and demonstrated the appropriate level of competence and commitment for their category of registration
- proved their ability and commitment to maintaining and improving their skills; and
- made a commitment to adhere to codes of conduct, practice, and ethics.

The Standard has been developed, and will be maintained, collaboratively by practitioners and experts from industry and academia and from the many different disciplines and specialisms that make up the cyber security profession, making it both comprehensive in its coverage of the range of specialisms and thorough in its treatment of the requirements for a professional in the sector.

Those who apply for professional registration undergo an independent peer assessment of their competence and commitment, to ensure that they meet or exceed the UK Standard for Cyber Security Competence. Individuals will be removed from the register if they breach its code of ethics or fail to demonstrate professionalism and commitment.

BENEFITS TO THE INDIVIDUAL

Professional registration:

- Shows that the individual concerned is working to achieve the cyber security needs of today and aspirations for tomorrow
- Indicates experience and expertise in the individual's chosen specialism(s) in cyber security to a nationally recognised standard of competence
- Guarantees the individual's commitment to professional standards such as the Council's codes of conduct, practice, and ethics
- Evidences a level of skill, knowledge and understanding of the profession, to a level indicated by the registration title and associated post-nominals
- Proves an ongoing commitment to continuing professional development to ensure their expertise and competence remain up to date and relevant
- Demonstrates that the individual belongs to a network of cyber security professionals which is respected and holds prestige
- Indicates a greater influence within their own organisation and industry
- Shows personal and professional integrity

- Indicates that the individual's competence and commitment is peer-reviewed
- Gives confidence and assurance to employers, clients and the public, nationally, and internationally
- Provides credibility with peers and improved career prospects and employability
- Is proof that professional skills have been acquired in a work-based environment – with critical awareness and valuable skills enhancing the individual's CV for career progression
- May increase the individual's earning potential.

In summary: professional registered status shows employers, clients and the public that the individual is committed to maintaining the knowledge, skills and competence required to meet the cyber security challenges and technological needs of today and tomorrow.

The prestige of the title enhances their CV, leading to wider employment options and career progression.

BENEFITS FOR EMPLOYERS

Having professionally registered staff with cyber security professional titles (Associate, Principal or Chartered):

- Adds value, often attracting higher fee rates
- Demonstrates compliance and commitment to high standards
- May enhance their employer's competitive edge

BENEFITS FOR CLIENTS

Clients may be reassured that professionally registered cyber security professionals:

- Are well-qualified and competent, with up-to-date cyber security expertise and knowledge
- Possess personal integrity, professional attributes, and academic qualifications
- Will contribute to their business success in a competitive environment
- Will abide by the Council's codes of conduct, practice, and ethics.

COMPETENCE AND COMMITMENT

WHAT IS CYBER SECURITY COMPETENCE?

Competence is defined as a professional's ability to carry out cyber security activities successfully within their Discipline / Specialism. This includes possessing the underpinning knowledge, understanding and experience within their Discipline / Specialism, knowledge and understanding of related Discipline / Specialism, the ability to communicate effectively at all levels, personal behaviour and approach, the ability to lead yet also know the limits of one's own abilities and when to request assistance.

For each professional registration title, a demonstration of competence is required in the following:

- Knowledge, Understanding and Experience
- Communication & Interpersonal Skills
- Integrity
- Professional Commitment
- Collaborative Leadership & Mentoring

The Council has published a paper on Specialisms identifying high level disciplines related to professional registration bodies and associated specialisms that are currently applicable to Cyber Security.

WHAT IS PROFESSIONAL COMMITMENT?

Cyber Security Professionals who wish to become Registered with the Council will be required to demonstrate both personal and professional commitment. Included within the overall requirement for competence it is mandatory that they demonstrate a set of values and conduct that not only maintains their own reputation, but also that of the profession.

The very nature of cyber is that it is constantly changing and evolving with new technological advances being made in noticeably short timescales. It is therefore essential that cyber security professionals demonstrate a commitment to maintaining their level of knowledge and understanding both within their Discipline / Specialism and related or new Discipline / Specialism that may arise. For this reason, all registered professionals may be required to demonstrate their professional commitment by keeping a record of their professional development and providing evidence of their continued practice at intervals of not less than 3 years.

Cyber is at the heart of all aspects of our daily lives whether at home, work, or recreation and, as such, the impact on individuals, businesses, and society as a whole when things go wrong, may be significant. It is essential, therefore, that anyone working at the heart of the Cyber Security Profession demonstrates a very high degree of integrity. Integrity in this instance uses the Cambridge Dictionary definition of Integrity, namely, *"the quality of being honest and having strong moral principles that you refuse to change."* This includes:

- Compliance with codes of conduct of their professional membership organisation.
- Compliance with the appropriate legal and regulatory requirements.

- Undertaking work in a way that considers the best interests of the individuals and businesses affected by the work.
- Continuing to maintain and enhance competence in relation to the underpinning knowledge, understanding and skills associated with the Discipline / Specialism.
- Recognising and actively promote inclusivity and diversity within the profession.
- Exercising responsibilities in an ethical manner.
- Adopting a security and safety minded approach that also takes into account environmental issues, where appropriate.
- Actively participating within the profession.

The Council has produced a code of ethics for professional membership organisations that become licensed bodies.

The Council has produced a Continuing Professional Development policy for all professionals registered members.

PROFESSIONAL REGISTRATION PROCESS

The professional review process closely aligns with that required by the Engineering Council and has been selected to have the minimal impact on existing registration organisations as the Council establishes itself. The process is currently in operation within the IET, the InstMC and the BCS and closely aligns to other professional membership organisations that are likely to become licensed members.

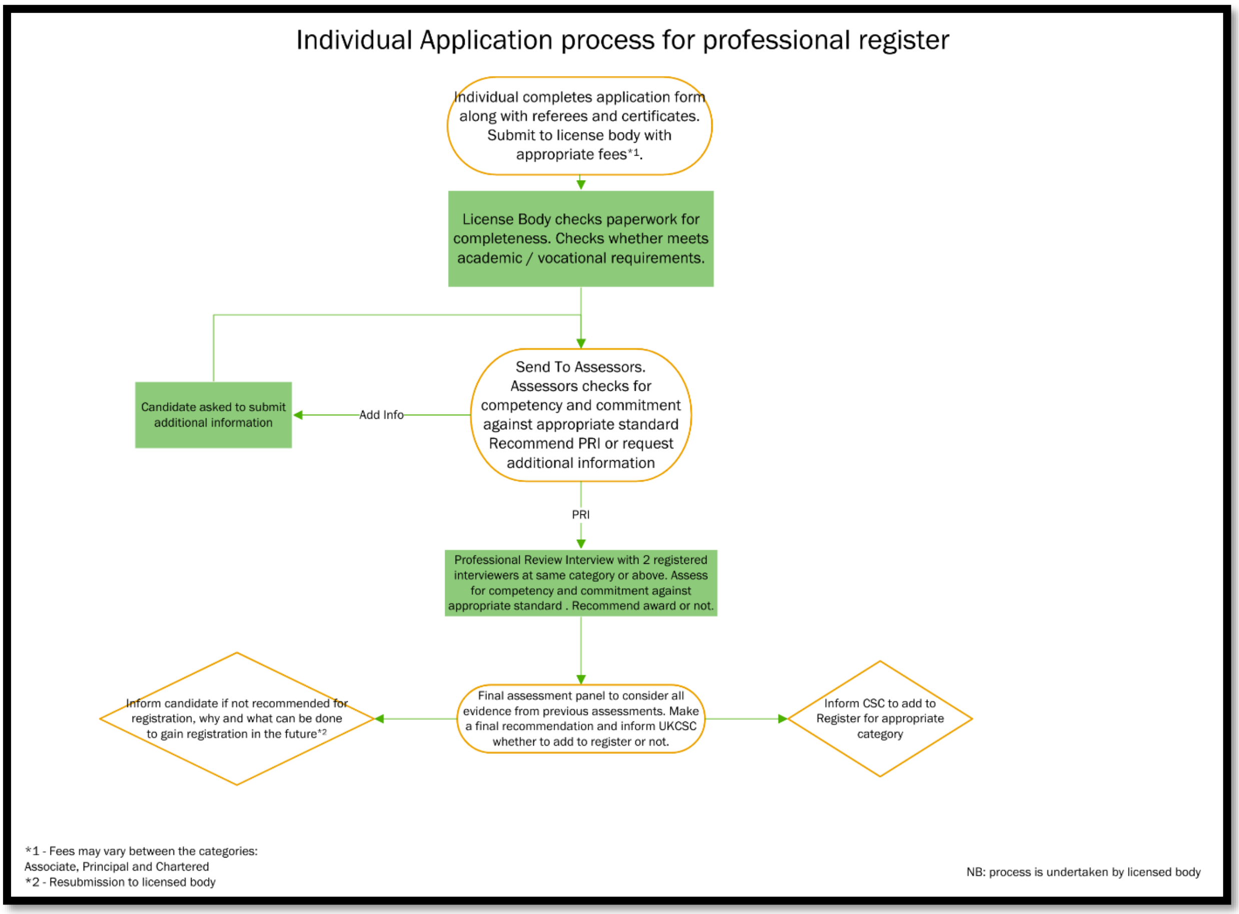
Individual Application process for professional register
Individual completes application form along with referees and certificates. Submit to license body with appropriate fees*1.
License Body checks paperwork for completeness. Checks whether meets academic / vocational requirements.
Send To Assessors. Assessors checks for competency and commitment against appropriate standard Recommend PRI or request additional information
Add Info
Candidate asked to submit additional information
PRI
Professional Review Interview with 2 registered interviewers at same category or above. Assess for competency and commitment against appropriate standard . Recommend award or not.
Final assessment panel to consider all evidence from previous assessments. Make a final recommendation and inform UKCSC whether to add to register or not.
Inform candidate if not recommended for registration, why and what can be done to gain registration in the future*2
Inform CSC to add to Register for appropriate category
*1 - Fees may vary between the categories: Associate, Principal and Chartered
*2 - Resubmission to licensed body
NB: process is undertaken by licensed body

Figure 3 - Individual Application Process for Professional Registration

Readers should note that separate documents cover the arrangements for licensing of organisations ("Licensed Bodies") to assess and recommend individuals as competent for inclusion on the register of cyber security professionals. These include the License Regulations.

REVALIDATION

Cyber Security Professionals may be required to revalidate their level of competence and commitment every three years in order to maintain their status and the use of the post nominals.

Should a candidate fail to revalidate or fails to meet the standard during revalidation they will be removed from the Register of Cyber Security Professionals until sufficient evidence is provided that they are able to evidence they are operating in accordance with the standard for the Cyber Security Professional.

The proposed process for revalidation is:

- Within one year following the 3rd anniversary of successful registration or recertification submit the following for assessment:

    - An updated CV (or similar) with specific reference to cyber security roles/responsibilities,
    - Evidence of CPD and Competency and Commitment within their Discipline / Specialism
    - References to support evidence

- The submission will be reviewed by approved cyber security assessors for validation
- The assessors may request further information, or an interview should any clarification be required.
- Once approved the revalidation date will be reset on the Register entry.

Should the revalidation process not be complete within one year of the original, or previous revalidation, then this will automatically trigger the registrant's removal from the Register of Cyber Security Professionals

MANAGEMENT OF THE REGISTER

Upon a recommendation from a Licensed Body and payment of the current fee, Registrants and their Licensing Body will be recorded in the relevant section of the Register. The Register will include relevant details of those individuals registered and may contain other information deemed appropriate by the Council (provided that such information is needed to administer the register and complies with current GDPR requirements). However, the Register will not be publicly searchable. Access to the Register will be provided to Licensed Bodies to verify the registration status of their individual members and others as needed to manage the registration process and adherence with License requirements.

Unless specified elsewhere in Regulations or by law, no person or other organisation shall be supplied with the record of any individual on the Register without the agreement of that individual.

Subject to the Council Regulations, only Individuals who are members of a Licensed Body which has a signed Licensing Agreement, may have their names added to or maintained on the Register.

The Council may at any time license an organisation which has met the relevant requirements. The Council may then add to the appropriate section of the Register any individual who, at the date of such licensing, is a Member of that Organisation in a category of membership requiring demonstration of competence and commitment, provided that the Council is satisfied that:

- The criteria applied at the time the individual was accepted into membership of that category was comparable to, or of a standard higher than, those criteria which would have had to have been satisfied if they had sought, at that time, registration in the appropriate grade; and

- The newly licensed body had, at the time the Individual was admitted and since, procedures in place for continuing professional development comparable to or of a standard higher than those required of Licensed Bodies.

An individual whose name is entered in the Register may, at their request and upon payment of a fee prescribed by the Council, receive a certificate of their achievement of the relevant title. This certificate will remain the property of the Council and shall be returned by its holder to the Council on written request from the Council's Chief Executive Officer or any person authorised by them.

The Council may hear an appeal from an individual who has been assessed as not meeting the relevant standard of competence by a Licensed Body. Such an appeal will be conducted in accordance with the procedures set out in the License Regulations, which shall provide for the right to an oral hearing and the right of representation.

Registration fees shall be payable in the manner prescribed in the Regulations. The Council reserves the right to amend the registration fees from time to time.

MAINTENANCE OF REGISTRATION

In order to remain on the Cyber Security Professional Register, Registrants are required to maintain their membership of a Licensed Body.

It is possible for an individual to maintain their registration if they cease to be a member of the Licensed Body through which they registered, under the following circumstances:

- The Organisation of which they were a Member has ceased to be a Licensed Body or has ceased to exist; or

- Their membership has lapsed or been cancelled, other than through expulsion or while the Registrant is the subject of disciplinary proceedings.

In such circumstances their registration will continue to be valid, provided that within twelve months of the cessation either:

- The former Licensed Body concerned is, in the opinion of the Council, able to provide and assess relevant continuing professional development, supervise, and enforce adequate disciplinary procedures and has become a Professional Affiliate with a Registration Agreement with a Licensed Body; or

- They become, or already are, a member of another licensed body and they arrange for their registration to be recorded through that body.

A Registrant who is expelled from membership of the Licensed Body through which they are registered shall cease to be a Registrant with effect from the conclusion of the disciplinary process (including any appeal either to the licensed body or to the Council). Once a Registrant has been informed that they are subject to disciplinary proceedings by the Licensed Body through which they are registered, they shall not seek to transfer their registration to another Licensed Body before the disciplinary process is complete.

In the event of a Registrant being removed from a Licenced Body for reason of conduct, the Licensed Body will inform the Council. The Council will remove the relevant Individual from the Register and mark the register such that other Licensed Bodies doing pre-application search can be alerted, so as to prevent the registrant from attempting to transfer their professional registration.

A Registrant may be suspended from the Register by the Licensed Body while disciplinary or conduct allegations are investigated. This suspension may last until the outcome of the disciplinary or conduct process outcome is known.

Where a Registrant is suspended for any reason, the Licensed Body shall inform the Council. Any suspensions for disciplinary reasons may be referred to the appropriate Council Board or Committee if deemed appropriate by the Licensed Body.

APPEAL BY AN INDIVIDUAL AGAINST LOSS OF REGISTRATION

The Council will consider an appeal from any Individual:

- Whose name appears on the Register; and
- Who is found, by a Licensed Body of which the Individual is a member, to have breached its code of conduct; and,
- Who consequently receives from that body a sanction, which would result in the Individual's removal from the Register.

An appeal to the Council may be made only once the disciplinary procedures of the Licensed Body or Member Body have been exhausted. Such an appeal will be conducted under the process set out in the Licence Regulations.

REGISTRATION REQUIREMENTS

UNDERPINNING KNOWLEDGE AND UNDERSTANDING

The Council is currently developing the Cyber Security Qualification Framework to improve the navigability of the cyber security learning and application landscape. Whilst this work is ongoing, there is a need to provide reference in outline to the expected level of knowledge, skill, experience, attitudes, and behaviours against the 3 professional registration titles that could be met through qualification, expertise, experience, or a mix of all. The table detailed below does not express qualification type, size, scope, content but merely provides alignment of the titles against varying educational, competence and skills frameworks.

	The Associate Cyber Security Professional (ACySyP) Standard	The Principal Cyber Security Professional (PCySyP) Standard	The Chartered Cyber Security Professional (CCySyP) Standard
Regulated Qualifications Framework (RQF)[1] and International Equivalency[2]	Level 3	Level 6	Level 7
Credit and Qualifications Framework for Wales (CQFW)[3]	Level 3	Level 6	Level 7
Scottish Credit and Qualifications Framework (SCQF)[4]	Level 6	Level 10	Level 11
Skills Framework for the Information Age[5]	Level 3	Level 5	Level 6
CIISec Skills Framework[6]	Level 3	Level 5	Level 6
NICE Cybersecurity Workforce Framework[7]	Entry	Intermediate	Advanced

Table 1 - Professional Registration Standard CSQF Requirements & Expected Equivalencies

[1] gov.uk/what-different-qualification-levels-mean/list-of-qualification-levels

[2] As defined by UK NARIC: naric.org.uk

[3] gov.wales/sites/default/files/publications/2018-02/level-descriptors.pdf

[4] scqf.org.uk/about-the-framework/interactive-framework/

[5] sfia-online.org/en/sfia-7/responsibilities

[6] ciisec.org/CIISEC/News/CIISec_release_the_latest_version_of_the_Skills_Framework_V_2_4.aspx

[7] niccs.cisa.gov/workforce-development/cyber-security-workforce-framework

THE ASSOCIATE CYBER SECURITY PROFESSIONAL (ACySyP) STANDARD

An Associate Cyber Security Professional will be able to demonstrate competence and commitment in all the areas below and provide appropriate evidence. The examples of evidence are intended as guidance to help identify activities that might demonstrate the required competence and commitment for Associate Cyber Security registration. They are intended as examples only, as the most appropriate evidence will vary with each individual role and their associated Discipline / Specialism. The list should not be considered as complete or prescriptive and other types of evidence may be valid.

An Associate Cyber Security Professional will have practical experience in a specific Discipline / Specialism in which they are a practitioner and as such should be operating at a level at which their professional expertise is being used effectively in their role.

Competence		**Examples of Evidence**
A - KNOWLEDGE, UNDERSTANDING & EXPERIENCE • **Associate Cyber Security Professionals should demonstrate that their knowledge, understanding, and experience relating to their Discipline / Specialism including some understanding of cyber security in its wider sense and should be able to demonstrate practical experience within their Discipline / Specialism.** *This competence is about the knowledge and application of expertise within their Discipline / Specialism with some knowledge across the wider cyber security Discipline / Specialism that allows for them to carry out their role effectively.*	**The individual shall demonstrate that they:** 1. Are engaged in a role or have practical experience of activities within their Discipline / Specialism	• Involved in a cyber security issue and the rectification of the appropriate solution. • Involved in a cyber security incident with remediation, carrying out appropriate actions. • Involved in the analysis of a cyber security problem and production of recommendations from the results. • Involvement in the evaluating of a cyber security requirement and documenting a requirements specification.
	2. Engaged in problem solving to meet a customer / organisational requirement.	• Involved in a Cyber Security Operational Centre. • Involved in implementing a cyber resilience plan. • Involved in testing the cyber security environment.
	3. Have contributed and implemented continuous improvement to cyber security.	• Evaluated and/or audited an organisation's cyber security polices and processes and implemented improvements. • Applied an improvement methodology to define and implement efficiencies across the organisation's cyber security operations.

B - COMMUNICATIONS & INTERPERSONAL SKILLS • **Associate Cyber Security Professionals should demonstrate that they have reasonable communications and interpersonal skills.** *This competence is about being able to communicate and discuss aspects of cyber security with their peers and managers within their organisation.*	**The individual shall demonstrate that they:** 1. Have the ability to discuss cyber security effectively to both technical non-technical audiences.	• Any activity where they were involved in communicating the necessary information related to a cyber security assignment.
	2. Have good personal and social skills and awareness of diversity and inclusivity	• Any activity that recognised equality, diversity or inclusivity as a factor related to cyber security.
	3. Have good oral and written communication skills.	• Delivery of any report, paper, presentation, or other talk related to their Discipline / Specialism. • Other activities where, communicating effectively with an audience was involved.
C - COLLABORATIVE MANAGEMENT, LEADERSHIP & MENTORING • **Associate Cyber Security Professionals should demonstrate that they understand the need to develop management skills and have carried out some supervisory activity within a cyber security environment.** *This competence is about being able to supervise in a cyber security environment. The competence should not only demonstrate the ability to supervise but to understand the need to develop management skills in an organisational context.*	**The individual shall demonstrate that they:** 1. Understand the management of resources in a cyber security environment.	• Supervised the delivery a minor cyber security project. • Supervised an activity within a cyber security project including effective communication with connected activities. • Supervised the delivery of a cyber security activity working with external partners.
	2. Able to supervise and develop people.	• Supervised cyber security training including responding to performance feedback. • Identified training requirements related to cyber security for self and others in order to implement a project or activity.
	3. Have an understanding of the need for organisational and time management skills	• Involvement in a cyber security activity where time was a significant constraint. • Assisted in the organisation of a cyber security activity.

	4. Understand the need for a professional and secure working environment	• Carried out a cyber security activity where the security of the environment had to be maintained. • Involved in developing policies or procedures to ensure a professional environment was established or maintained.
D - INTEGRITY • **Associate Cyber Security Professionals should demonstrate that they understand and apply integrity, morals, and ethical values.** *This competence is about demonstrating a core commitment to the cyber security profession. Those involved in the cyber security profession need to hold the trust of society given the potential to apply security skills to cause as well as reduce harm. This competence is also about demonstrating their commitment to complying with codes of conduct, adherence to standards and acting in accordance with legal and regulatory requirements.*	**The individual shall demonstrate that they:** 1. Have personal and professional honesty and integrity.	• Provide an example where their cyber security responsibilities were carried out in an ethical manner. • Provide an example where unethical behaviour / poor practice in others, was challenged. • Where monitoring of their own performance produced an awareness of their own professional limitations. • Where privacy and ethical considerations were respected whilst performing their cyber security activities whilst adhering to organisation policies and objectives.
	2. Comply with codes of conduct of their professional membership organisation	• Any incident where confidential whistleblowing may have been carried out. • The identification of a code of conduct requirement that was particularly relevant to a cyber security incident or activity.
	3. The Understanding and compliance with appropriate legal and regulatory requirements.	• An activity where legal and regulatory requirements had an impact on the work, including how these requirements were complied with.
	4. Able to identify and implement appropriate standards	• Any activity where conformance to standards related a specific cyber security activity was carried out. • Any activity where non cyber security standards were implemented as part of a cyber security activity and how conformance was assessed.
E - PERSONAL COMMITMENT	**The individual shall demonstrate that they:**	• Provision of a log of existing CPD activities and a plan for future CPD activities aligned to either changes in role or advancements in technology.

• **Associate Cyber Security Professionals should demonstrate that they carry out and plan for continued development of themselves and the cyber security profession.** *This competence is about demonstrating a commitment to continued development of their own knowledge and understanding for their Discipline / Specialism, improving their knowledge and skills of the wider cyber security profession, understanding, and adapting to advances in technology and to the promotion of the profession.*	1. Carry out and record Continuing Professional Development (CPD).	
	2. Actively participate and promote the cyber security profession.	• Engagement in activities associated with the promotion of the cyber security profession.
	3. Maintain a working knowledge of technological advancements	• Carrying out activities to identify advances related to their Discipline / Specialism.

Table 2 - The Associate Cyber Security Professional Standard for Competence & Commitment

THE PRINCIPAL CYBER SECURITY PROFESSIONAL (PCySyP) STANDARD

A Principal Cyber Security Professional will be able to demonstrate competence and commitment in all the areas below and provide appropriate evidence. The examples of evidence are intended as guidance to help individuals identify activities that might demonstrate the required competence and commitment for Principal Cyber Security registration. They are intended as examples only as the most appropriate evidence will vary with each individual role and their associated Discipline / Specialism. The list should not be considered as complete and other types of evidence may be valid.

A Principal Cyber Security Professional will have practical experience in a specific Discipline / Specialism at which they are an expert practitioner and have experience in other Discipline / Specialism and as such should be operating at a level where their professional expertise may reasonably be sought to contribute to the development of their specific Discipline / Specialism.

Competence		**Examples of Evidence**
A - KNOWLEDGE, UNDERSTANDING & EXPERIENCE • **Principal Cyber Security Professional should demonstrate their knowledge, understanding and experience relating to their Discipline / Specialism including experience of cyber security in another Discipline / Specialism** *This competence is about the depth of knowledge and application of expertise within their own Discipline / Specialism with some knowledge and expertise across the wider cyber security Discipline / Specialism that allows for the practical implementation of solutions to address cyber security challenges. This will include understanding the interaction and inter-relationship between technology, people, physical environment, and risk.*	**The individual shall demonstrate that they:** 1. Are engaged in a role or have practical experience of activities that have a degree of complexity within their Discipline / Specialism	• Managing the investigation of a cyber security issue, identifying workable solutions and selection of most appropriate solution. • Responded to a cyber security incident, assisted in identifying appropriate actions and subsequent implementation of a remediation plan. • Investigating a cyber security problem, carrying out analysis and recommending the results. • Leading the evaluating of a cyber security requirement and developing a requirements specification.
	2. Applied problem solving tools and techniques in meeting customer / organisational requirements.	• Involved in a new business operational requirements analysis and the selection of appropriate cyber security controls. • Involved in managing a Cyber Security Operational Centre for a customer / organisation. • Managed the implementation of a cyber resilience plan. • Involved in establishing a test and reference facility for a customer / organisational operational environment.

	3.Have planned or delivered continuous improvement to cyber security.	- Evaluated and/or audited an organisation's cyber security objectives and implemented improvements. - Applied an improvement methodology to define and implement efficiencies across the organisation's cyber security operations.
B - COMMUNICATIONS & INTERPERSONAL SKILLS - **Principal Cyber Security Professionals should demonstrate that they have appropriate communications and interpersonal skills to fulfil their role within their organisation with those who may have little or no knowledge of cyber security.** *This competence is about being able to communicate and discuss aspects of cyber security within their organisation. This includes the ability to discuss and communicate cyber security, with attention to detail, to those with little cyber security knowledge.*	**The individual shall demonstrate that they:** 1. Have the ability to explain cyber security effectively to non-technical audiences.	- Any activity where they communicated all the necessary information in order to carry out an appropriate cyber security assignment within their organisation.
	2. Explain cyber security advice and direction in a way that is clearly understood by the intended audience	- How a cyber security problem was communicated using the language of the organisation. - How a business requirement and priorities were translated into cyber security activities and actions. - The preparation of reports or specifications as part of a bidding process for a cyber security product or service.
	3. Have good personal and social skills that demonstrate empathy, diversity, and inclusivity	- The creation of or enhancing a productive working relationship within an organisation or with a customer. - By taking a variety of perspectives and approaches and developing a collaborative cyber security solution. - Working within a team to develop collective cyber security goals with a challenging team dynamic - Any activity that recognised equality, diversity, or inclusivity as a factor during a cyber security incident.
	4. Have good oral and written communication skills for both technical and non-technical audiences	- Delivery of cyber security advice and direction in a way that was clearly understood by the intended audience. - Contributed to a scientific cyber security paper or article utilising knowledge and expertise from the Discipline / Specialism.

		• Presenting a cyber security remediation plan.
C - COLLABORATIVE MANAGEMENT, LEADERSHIP & MENTORING • **Principal Cyber Security Professionals should demonstrate that they have developed management skills and are able to demonstrate their ability to lead groups and individuals in a personal, technical, or business cyber security environment.** *This competence is about being able to manage individuals and teams in a cyber security context and in a number of environments. The competence should not only demonstrate the ability to lead in an organisational context but also the ability to contribute to the wider knowledge and understanding of their cyber security Discipline / Specialism.*	**The individual shall demonstrate that they:** 1. Are able to manage resource, people, budgets in a cyber security environment.	• Responsible for delivering a cyber security activity demonstrating the management of associated risk. • Management of an organisational cyber security team especially during a cyber security incident. • Managing a cyber security project from requirements through to implementation, • Leading the execution and delivery of a cyber security project with external partners.
	2. Able to lead, manage and develop people.	• Managing cyber security teams and individuals with specialist training requirements. • Delivering effective cyber security training / education in their Discipline / Specialism. • Managing a cyber security training team, monitoring the training provided, including performance feedback. • Led an ad-hoc team including non cyber security personnel in responding to a cyber security incident.
	3. Have good organisational and time management skills	• Established a new cyber security team within an organisation including measures to monitor effectiveness. • Managed cyber security activities in an effective way that improved the overall organisational security posture relative to the risk. • Managed the setting and delivery of cyber security activities to deadlines.
	4. Maintain a professional and secure working environment	• Ensured cyber security activities were managed in a way that considered the best interests of the individuals carrying out the work. • How a secure environment was established to manage a cyber security activity for a diverse set of individuals.
D - INTEGRITY	**The individual shall demonstrate that they:**	• Provide an example where their cyber security responsibilities were carried out in an ethical manner.

• **Principal Cyber Security Professionals should demonstrate that they have high levels of integrity, morals, and ethical values.** *This competence is about demonstrating a core commitment to the cyber security profession. Those involved in the cyber security profession need to hold the trust of society given the potential to apply security skills to cause as well as reduce harm. This competence is also about demonstrating their commitment to complying with codes of conduct, adherence to standards and acting in accordance with legal and regulatory requirements.*	1. Have personal and professional honesty and integrity.	• Provide examples where unethical behaviour / poor practice in others, was challenged. • Where monitoring of their own performance produced an awareness of their own professional limitations. • Where privacy and ethical considerations were respected whilst performing their cyber security activities whilst adhering to organisation policies and objectives. • Management of an issue where privacy and ethical issues gave rise to an impact on trust.
	2. Comply with codes of conduct of their professional membership organisation	• The escalation of 'prominent issues' discovered that may have included confidential whistleblowing. • The Identification of specific aspects of the code that were particularly relevant to a cyber security incident or activity.
	3. The understanding and compliance with appropriate legal and regulatory requirements.	• The identification of legal requirements within which they had to work, including how compliance was met. • Identification of non-UK legal & regulatory requirements during a cyber security activity. • Activities where legal frameworks covering transfers of personal data from UK to non-UK countries were identified and how compliance was achieved.
	4. Able to identify and implement appropriate standards	• Identification, implementation, and conformance to standards related a specific cyber security activity. • Identification of non cyber security standards that were implemented as part of a cyber security activity and how conformance was assessed.
E - PERSONAL COMMITMENT	**The individual shall demonstrate that they:**	• Provision of a log of existing CPD activities and a plan for future CPD activities aligned to either changes in role or advancements in technology.

• **Principal Cyber Security Professionals should demonstrate that they are committed to the continued development of themselves and the cyber security profession.** *This competence is about demonstrating a commitment to continued development of their own knowledge and understanding for their Discipline / Specialism, improving their knowledge and skills of the wider cyber security profession, understanding, and adapting to advances in technology and to the promotion of the profession.*	1. Carry out and record Continuing Professional Development (CPD).	
	2. Actively participate and promote the cyber security profession.	• Engagement in activities associated with the promotion of the cyber security profession. • Engagement in activities associated supporting charities and other organisations that do not have a cyber security capability. • Attendance at non cyber security events to promote the profession.
	3. Maintain a working knowledge of technological advancements, threat space	• Carrying out horizon scanning activities for future cyber security trend watch related to their Discipline / Specialism. • The management of a cyber security alerting function at the organisational level.

Table 3 - The Principal Cyber Security Professional Standard for Competence & Commitment

THE CHARTERED CYBER SECURITY PROFESSIONAL (CCySyP) STANDARD

A Chartered Cyber Security Professional will be able to demonstrate competence and commitment in all the areas below and provide appropriate evidence. The examples of evidence are intended as guidance to help individuals identify activities that might demonstrate the required competence and commitment for Chartered Cyber Security registration. They are intended as examples only as the most appropriate evidence will vary with each individual role and their associated Discipline / Specialism. The list should not be considered as complete and other types of evidence may be valid.

A Chartered Cyber Security Professional will have significant practical experience in several Discipline / Specialism, though may still have a particular Discipline / Specialism at which they may be an acknowledged expert and as such should be operating at a level where their professional opinion may reasonably be sought to contribute to the development of the overall cyber security profession.

Competence		Examples of Evidence
A - KNOWLEDGE, UNDERSTANDING & EXPERIENCE • **Chartered Cyber Security Professionals should demonstrate their knowledge, understanding and experience relating to their Discipline / Specialism including understanding of cyber security in its widest sense and should be able to demonstrate practical experience across a number of security Discipline / Specialism.** *This competence is about the depth of knowledge and application of expertise not only within their own Discipline / Specialism but across a number of related Discipline / Specialism that allows for the development of novel and unexpected solutions to address cyber security challenges. This will include understanding the interaction and inter-relationship*	**The individual shall demonstrate that they:** 1. Have led, managed, or carried out activities that have a degree of complexity across a number of Discipline / Specialism and understand how skills should be applied across a number of projects and to different environments	• Investigating a complex cyber security issue, identifying workable solutions and selection of most appropriate solution. • Responding to a significant cyber security incident, identifying appropriate actions and implementation of a remediation plan. • Researching a complex cyber security problem, carrying out analysis and evaluating the results. • Evaluating a cyber security requirement, developing a requirements specification, analysing the market, selecting and implementing the solution. • Secures the scene, captures and processes evidence in accordance with recognised practice and procedure to demonstrate repeatability in legal proceedings" (E.g., ACPO guidelines)
	2. Have applied analytical problem solving in meeting customer / organisational requirements.	• Led the design and development of a cyber security strategy and plan linked to the organisations vision and business objectives.

between technology, people, physical environment, and risk. This will include roles or activities that have a degree of complexity across a number of Disciplines / Specialisms and required analytical problem solving in meeting customer / organisational requirements.		• Evaluated new business operational requirements, developed, agreed, and implemented appropriate cyber security controls. • Evaluating and establishing a Cyber Security Operational Centre for a customer / organisation. • Developing and establishment of a cyber resilience plan including consideration of people, processes, physical and technological requirements. • Researching, evaluating, and establishing a test and reference facility for a customer / organisational operational environment. • Development of a strategic cyber security plan from scratch for an organisation.
	3. Have led, managed, or coordinated continuous improvement to cyber security.	• Evaluated and/or audited an organisations cyber security strategy and implemented improvements. • Applied an improvement methodology to define and implement efficiencies across the organisations cyber security operations.
B - COMMUNICATIONS & INTERPERSONAL SKILLS • **Chartered Cyber Security Professionals should demonstrate that they have effective communications and interpersonal skills to operate at all levels**	**The individual shall demonstrate that they:** 1. Have the ability to question and listen, summarise and explain cyber security appropriately.	• Any activity where understanding and eliciting all the necessary information in order to carry out an appropriate cyber security business/risk balance and advise accordingly.

within and without an organisation, with their peers and those who have little or no knowledge of cyber security. *This competence is about being able to communicate and discuss all aspects of cyber security at all levels both within and without an organisation. This includes the ability to discuss and communicate cyber security, with attention to detail, to those with little or no knowledge and to convert the technical language of cyber into that understood by the organisation.*	2. Provide and explain cyber security advice, direction and/or expert opinion, in a way that can clearly be understood by the intended audience	• How a cyber security problem was communicated, analysed and recommended using the language of the organisation and in doing so subsequently affected a positive change. • How a business requirement and priorities were translated into cyber security consequences and agreed mitigations. • The preparation of reports, drawings, budgets, and specifications etc. as part of a bidding process for a cyber security product or service.
	3. Have good personal and social skills that demonstrate empathy, diversity, and inclusivity	• The creation, maintaining and enhancing productive working relationships within an organisation or with a customer including a degree of conflict resolution. • Demonstrating creativity by taking a variety of perspectives, taking account of unpredictable adversary, threat behaviours and approaches and developing collaborative solutions. • Working with a team to develop collective cyber security goals during a changing interpersonal situation • Provision of support during a cyber security incident ensuring the needs of others were met, especially from a diversity and inclusion perspective.
	4. Have excellent oral and written communication skills for both technical and non-technical audiences	• Provision and explanation of cyber security advice, direction and/or expert opinion, in a way that was clearly understood by the intended audience. • Contributing to a published scientific cyber security paper or article as an author. • Presenting a published cyber security academic paper at an academic conference.
C - COLLABORATIVE MANAGEMENT, LEADERSHIP & MENTORING	**The individual shall demonstrate that they:**	• Being accountable or having responsibility for delivering a complex cyber security activity with significant risk.

• **Chartered Cyber Security Professionals should demonstrate that they have developed effective management skills and are able to demonstrate their ability to lead and mentor groups and individuals in a personal, technical, or business cyber security environment.** *This competence is about being able to establish, manage and mentor individuals and teams in a cyber security context and in a number of challenging environments. The competence should not only demonstrate the ability to lead in an organisational context but also the ability to lead or exert influence that contributes to the wider knowledge and understanding of cyber security.*	1. Are able to manage resource, people, budgets in complex and/or high-pressure cyber security environments.	• The successful management of an organisational cyber security team during a major incident. • The planning and budgeting of a cyber security project from concept through to commissioning, • The planning, execution, and delivery of a complex cyber security research project with external research partners. • Led teams conducting investigations using forensic techniques and tools. Experienced in using multiple forensic tools and techniques
	2. Able to lead, manage and develop people through coaching and mentoring. Creates and leads formal or informal teams and / or creates collaborative links with teams. Provides support and feedback to encourage and develop colleagues. Advises and influences others.	• Supervising cyber security researchers and assisting in getting the research published. • Developing and delivering cyber security education at MSc level or in some other way exerting influence that contributes significantly to the field). • Identifying and developing both formal and informal cyber security training plans teams / individuals and providing the time and opportunity to undertake the training, including performance feedback. • Where human behaviours in the context of cyber risk and risk related decisions were identified and managed effectively.
	3. Have excellent organisational and time management skills	• Established a new cyber security team / organisation within in a high-pressure environment that was working effectively within the time constraints allowed. • Prioritised a number of cyber security activities in a way that delivered the most effective security posture in the minimum amount of time relative to the risk observed. • The consistent setting and meeting of deliverable deadlines in cyber security activities

	4. Maintain a productive, professional, and secure working environment	• How cyber security activities were carried out in a way that considered the best interests of the individuals and organisations affected by the work. • How a secure collaboration space was established to develop a cyber security solution for a diverse set of stakeholders.
D - INTEGRITY • **Chartered Cyber Security Professionals should demonstrate that they have the highest level of integrity, morals, and ethical values.** *This competence is about demonstrating a core commitment to the cyber security profession. Those involved in the cyber security profession need to hold the trust of society given the potential to apply security skills to cause as well as reduce harm. This competence is also about demonstrating their commitment to complying with codes of conduct, adherence to standards and acting in accordance with legal and regulatory requirements.*	**The individual shall demonstrate that they:** 1. Have personal and professional honesty and integrity.	• Provide examples of carrying out their cyber security responsibilities in an ethical manner. • Provide examples where unethical behaviour / poor practice in others, especially where this might cause harm, was challenged and managed. • Where diligence in their own performance and advice produced an awareness of their professional limitations. • Identifying and respecting privacy and ethical considerations raised during their cyber security activities whilst adhering to organisation policies and objectives. • Where an awareness of privacy and ethics issues gave rise to an impact on trust and confidence and how this was managed.
	2. Comply with codes of conduct of their professional membership organisation	• The escalation of 'prominent issues' discovered that required confidential whistleblowing within the business, a client business, or externally to law enforcement. • Identifying specific aspects of the code that are particularly relevant to either the current or previous cyber security role.
	3. Understand and comply with the appropriate	• Identification of legal parameters within which a cyber security professional had to work, that required compliance.

	legal and regulatory requirements.	• Identification of non-UK legal & regulatory requirements during a cyber security activity that required compliance. • Activities where legal frameworks covering transfers of personal data from UK to non-UK countries. • Where cyber security activities for Defence / government that would otherwise be considered breaches of law, but which were made lawful were conducted by state agencies principally in the interests of national security, and for the prevention and detection of serious crime.
	4. Are able to identify and implement appropriate standards	• Identification, implementation, and conformance to appropriate standards during a cyber security activity. • Identification of applicable non cyber security standards that were implemented as part of a cyber security activity.
E - PERSONAL COMMITMENT • **Chartered Cyber Security Professionals should demonstrate that they are committed to the continued development of themselves and the cyber security profession.** *This competence is about demonstrating a commitment to continued development of their own knowledge and understanding for their Discipline / Specialism, improving their knowledge and skills of the wider cyber security profession, understanding, and adapting to advances in technology and to the promotion of the profession.*	**The individual shall demonstrate that they:** 1. Carry out and record Continuing Professional Development (CPD).	• Provision of a log of existing CPD activities and a plan for future CPD activities aligned to either changes in role or advancements in technology.
	2. Actively participate and promote the cyber security profession.	• Engagement in activities associated with the promotion of the cyber security profession to schools. • Engagement in activities associated supporting charities and other organisations that do not have a cyber security capability. • Attendance at events that are not cyber security focussed where promotion through speaking or networking about cyber security was achieved.

	3. Maintain a working knowledge of technological advancements, threat space	• Carrying out horizon scanning activities for future cyber security trend watch. • The establishment and maintenance of a cyber security alerting function at either the organisational or personal level.

Table 4 - The Chartered Cyber Security Professional Standard for Competence & Commitment

COMPARISON OF STANDARDS

Associate	Principal	Chartered
Competence & Commitment Standard for Associate Cyber Security Professionals An Associate Cyber Security Professional will have practical experience in a specific Discipline / Specialism at which they are a practitioner and as such should be operating at a level where their professional expertise is being used effectively in their role. Associate Cyber Security Professionals shall demonstrate: • Their knowledge, understanding and experience relating to their Discipline / Specialism including some understanding of cyber security in its wider sense and should be able to demonstrate practical experience within their Discipline / Specialism. • They have reasonable communications and interpersonal skills. • They understand the need to develop management skills and have carried out some supervisory activity within a cyber security environment.	**Competence & Commitment Standard for Principal Cyber Security Professionals** A Principal Cyber Security Professional will have practical experience in a specific Discipline / Specialism at which they are an expert practitioner and have experience in other Disciplines / Specialisms and as such should be operating at a level where their professional expertise may reasonably be sought to contribute to the development of their specific Discipline / Specialism. Principal Cyber Security Professionals shall demonstrate: • Their knowledge, understanding and experience relating to their Discipline / Specialism including experience of cyber security in another Discipline / Specialism. • That they have appropriate communications and interpersonal skills to fulfil their role within their organisation with those who may have little or no knowledge of cyber security. • That they have developed management skills and are able to demonstrate their ability to lead groups and individuals in a	**Competence & Commitment Standard for Chartered Cyber Security Professionals** A Chartered Cyber Security Professional will have significant practical experience in several Disciplines / Specialisms, though may still have a particular Discipline / Specialism at which they may be an acknowledged expert and as such should be operating at a level where their professional opinion may reasonably be sought to contribute to the development of the overall cyber security profession. Chartered Cyber Security Professionals shall demonstrate: • Their knowledge, understanding and experience relating to their Discipline / Specialism including understanding of cyber security in its widest sense and should be able to demonstrate practical experience across a number of security Disciplines / Specialisms. • They have effective communications and interpersonal skills to operate at all levels within and without an organisation, with their peers and those who have little or no knowledge of cyber security. • They have developed effective management skills and are able to

• They understand and apply integrity, morals, and ethical values. • They carry out and plan for continued development of themselves and the cyber security profession.	personal, technical, or business cyber security environment. • That they have high levels of integrity, morals, and ethical values. • That they are committed to the continued development of themselves and the cyber security profession.	demonstrate their ability to lead and mentor groups and individuals in a personal, technical, or business cyber security environment. • They have the highest level of integrity, morals, and ethical values. • They are committed to the continued development of themselves and the cyber security profession.
A. Knowledge, Understanding & Experience Associate Cyber Security Professionals shall use their knowledge, understanding and experience relating to their Discipline / Specialism including some understanding of cyber security in its wider sense and should be able to demonstrate practical experience within their Discipline / Specialism. The individual shall demonstrate that they: • Are engaged in a role or have practical experience of activities within their Discipline / Specialism. • Engaged in problem solving to meet a customer / organisational requirement.	**A. Knowledge, Understanding & Experience** Principal Cyber Security Professionals should demonstrate their knowledge, understanding and experience relating to their Discipline / Specialism including experience of cyber security in other Disciplines / Specialisms. The individual shall demonstrate that they: • Are engaged in a role or have practical experience of activities that have a degree of complexity within their Discipline / Specialism. • Applied problem solving tools and techniques in meeting customer / organisational requirements.	**A. Knowledge, Understanding & Experience** Chartered Cyber Security Professionals should demonstrate their knowledge, understanding and experience relating to their Discipline / Specialism including understanding of cyber security in its widest sense and should be able to demonstrate practical experience across a number of security Disciplines / Specialisms. The individual shall demonstrate that they: • Have led, managed, or carried out activities that are complex across a number of Disciplines / Specialisms. • Applied analytical problem solving in meeting customer / organisational requirements. • Have led, managed, or coordinated continuous improvement to cyber security.
B. Communications & Interpersonal Skills	**B. Communications & Interpersonal Skills**	**B. Communications & Interpersonal Skills**

Associate Cyber Security Professionals should demonstrate that they have reasonable communications and interpersonal skills. The individual shall demonstrate that they: • Have the ability to discuss cyber security effectively to both technical and non-technical audiences. • Have good personal and social skills and awareness of diversity and inclusivity. • Have good oral and written communication skills.	Principal Cyber Security Professionals should demonstrate that they have appropriate communications and interpersonal skills to fulfil their role within their organisation with those who may have little or no knowledge of cyber security. The individual shall demonstrate that they: • Have the ability to explain cyber security effectively to technical and non-technical audiences. • Explain cyber security advice and direction in a way that is clearly understood by the intended audience. • Have good personal and social skills that demonstrate empathy, diversity, and inclusivity. • Have good oral and written communication skills for both technical and non-technical audiences	Chartered Cyber Security Professionals should demonstrate that they have effective communications and interpersonal skills to operate at all levels within and without an organisation, with their peers and those who have little or no knowledge of cyber security. The individual shall demonstrate that they: • Have the ability to question and listen, summarise and explain cyber security appropriately. • Provide and explain cyber security advice, direction and/or expert opinion, in a way that can clearly be understood by the intended audience. • Have good personal and social skills that demonstrate empathy, diversity, and inclusivity. • Have excellent oral and written communication skills for both technical and non-technical audiences.
C. Collaborative Management, Leadership & Mentoring Associate Cyber Security Professionals should demonstrate that they understand the need to develop management skills and have carried out some supervisory activity within a cyber security environment	**C. Collaborative Management, Leadership & Mentoring** Principal Cyber Security Professionals should demonstrate that they have developed management skills and are able to demonstrate their ability to lead groups and individuals in a personal, technical, or business cyber security environment.	**C. Collaborative Management, Leadership & Mentoring** Chartered Cyber Security Professionals should demonstrate that they have developed effective management skills and are able to demonstrate their ability to lead and mentor groups and individuals in a

The individual shall demonstrate that they: • Understand the management of resources in a cyber security environment. • Able to supervise and develop people. • Have an understanding of the need for organisational and time management skills. • Able to identify and implement appropriate standards.	The individual shall demonstrate that they: • Are able to manage resource, people, budgets in a cyber security environment. • Able to lead, manage and develop people. • Have good organisational and time management skills. • Maintain a professional and secure working environment.	personal, technical, or business cyber security environment. The individual shall demonstrate that they: • Are able to manage resource, people, budgets in complex and/or high-pressure cyber security environments. • Able to lead, manage and develop people through coaching and mentoring. • Have excellent organisational and time management skills. • Maintain a productive, professional, and secure working environment.
D. Integrity Associate Cyber Security Professionals should demonstrate that they understand and apply integrity, morals, and ethical values. The individual shall demonstrate that they: • Have personal and professional honesty and integrity. • Comply with codes of conduct of their professional membership organisation. • The Understanding and compliance with appropriate legal and regulatory requirements. • Able to identify and implement appropriate standards.	**D. Integrity** Principal Cyber Security Professionals should demonstrate that they have high levels of integrity, morals, and ethical values. The individual shall demonstrate that they: • Have personal and professional honesty and integrity. • Comply with codes of conduct of their professional membership organisation. • The Understanding and compliance with appropriate legal and regulatory requirements. • Able to identify and implement appropriate standards.	**D. Integrity** Chartered Cyber Security Professionals should demonstrate that they have the highest level of integrity, morals, and ethical values. The individual shall demonstrate that they: • Have personal and professional honesty and integrity. • Comply with codes of conduct of their professional membership organisation. • Understand and comply with the appropriate legal and regulatory requirements. • Are able to identify and implement appropriate standards.

E. Personal Commitment	**E. Personal Commitment**	**E. Personal Commitment**
Associate Cyber Security Professionals should demonstrate that they carry out and plan for continued development of themselves and the cyber security profession. The individual shall demonstrate that they: • Carry out and record Continuing Professional Development (CPD). • Actively participate and promote the cyber security profession. • Maintain a working knowledge of technological advancements.	Principal Cyber Security Professionals should demonstrate that they are committed to the continued development of themselves and the cyber security profession. The individual shall demonstrate that they: • Carry out and record Continuing Professional Development (CPD). • Actively participate and promote the cyber security profession. • Maintain a working knowledge of technological advancements and threat space.	Chartered Cyber Security Professionals should demonstrate that they are committed to the continued development of themselves and the cyber security profession. The individual shall demonstrate that they: • Carry out and record Continuing Professional Development (CPD). • Actively participate in research and promote the cyber security profession. • Maintain a working knowledge of technological advancements and threat space.

Table 5 - Comparison of the Standards for Professional Competence & Commitment

CONTINUING PROFESSIONAL DEVELOPMENT (CPD)

INTRODUCTION

In today's world, it is vital that professionals remain competent and, therefore, are required to demonstrate that their knowledge and professional skills are being kept current. This is particularly important because of the continual advances and growth in cyber and cyber security in particular.

This growth means that there is an increasing need to understand the changes and implement advances as they are identified, developed, and become mainstream. This is particularly important whether considering the system as a whole or interfacing with other disciplines providing non-functional requirements. It requires the individual to develop and maintain up-to-date knowledge and skills to ensure they can meet the needs of the evolving professional requirements.

The Council acknowledges that it is the responsibility of individuals to ensure the systematic maintenance, improvement and broadening of knowledge and skills, in turn to ensuring continuing competence throughout their career; that is to say, it is the responsibility of individuals to undertake continuing professional development (CPD).

CPD has several purposes, which will vary in relation to the individual’s own circumstances, needs and career progression. It can also take a variety of forms. At its heart is experiential learning through the challenges and opportunities of working life. This is supplemented by interaction with others such as colleagues, customers and suppliers, and professionals from other disciplines - all leading to enhanced competence.

It may also be supplemented by structured activities such as courses, distance learning programmes, private study, preparation of papers and presentations, mentoring, involvement in professional body activities, or relevant voluntary work. The list is not exhaustive and individuals are best placed to determine their own development needs and how to meet them.

There may also be requirements from the employer; a particular qualification or from the Licensed Body of which the individual is a member. Existing professional bodies often promote the planning of structured CPD that incorporates a balance of sources including training, work experience, academic study, volunteering, events/seminars, and self-study. CPD records prepared for other purposes may also be acceptable evidence of CPD.

Examples include records produced for other professional institutions/organisations, company training, development, and appraisal processes. It is for the licensed body to specify any particular requirements for the format of CPD records/submissions, in line with the license requirements for monitoring.

REGISTRANTS AND CPD

One of the main functions of the Council is the development and professionalisation of the cyber security profession. As such, the Council promotes and supports the professional development of its registrants. It will be mandatory for all individual practitioners who are Registered with the Council to undertake and record continuing professional development (CPD). This requirement will be flowed down and managed through the license with

Licensed Bodies. The Council also sets an expectation that Licensed Bodies will mandate CPD among the cyber security practitioners within their memberships, regardless of registration status.

All successful applicants who become a Registrant, through assessment and recommendation by any organisation licensed by the Council, commit to maintaining and enhancing their competence by undertaking structured and unstructured CPD. It will be a requirement that the individuals maintain membership of a Licensed Body in order to support their CPD.

Organisations licensed by the Council are committed to advising members and to support their CPD in a number of ways. Examples include the provision of structured programmes, guidance, resources, and training programmes.

UK CYBER SECURITY COUNCIL CPD POLICY STATEMENT

The Council's CPD Policy Statement (see below) explains in more detail the nature, purpose, and value of CPD, and explains the support that members should expect from their licensed organisation.

CPD is accepted across most professions as 'the systematic acquisition of knowledge and skills, and the development of personal qualities, to maintain and enhance professional competence.' Regardless of their registered status, all individual members of organisations licensed by the Council have a mandatory obligation to maintain their competence through CPD, and to support the learning of the wider community. Council - registered individuals must commit to the planning, recording, and making available for reporting of their own CPD.

This obligation underpins the value of the professional registration titles of the cyber security profession, as well as enabling society to have confidence in the profession.

Employers or experienced colleagues will often play a significant part in this process, but individuals should be responsible and proactive in planning and in seeking professional development opportunities.

While it is expected that cyber security professionals will undertake CPD on a regular, on-going basis, it is accepted that some activities may occur without deliberate planning or recording of activities.

Whatever its purpose or nature, learning through CPD should be reflective and should, where possible, relate to specific objectives even if these are only to maintain their professional cyber security competence. Having a regularly reviewed development plan will facilitate learning, although there will always be a place for unplanned activities. Recording and reflection on activities, and the outcomes they have had in terms of individual learning, is a valuable process for turning learning into competence.

The Council expects that a documented CPD record is a requirement of maintaining registration. The Council further expects that this record is submitted (in a suitable format) for monitoring as required by the licensed body of which the registrant is a member.
In line with accepted good practice, the CPD activity must be related and relevant to the specialism of the registered professional, resulting in improved behaviour and practice.

The Council does not mandate a particular CPD system. It requires that licensed bodies should maintain a structured approach in line with the needs of its members and their employers. This must include regular monitoring, which may include sampling of members CPD records to assure compliance. Licensed bodies will be required to demonstrate that they provide both appropriate support and guidance for members' CPD, and a suitable compliance monitoring process, which will be part of regular quality assurance audits

SUMMARY OF REQUIREMENTS

Licensed Bodies

All bodies licensed by the Council will:

a. Meet the requirements and criteria set by the Council in their Policy for CPD.
b. Support registered individuals with their CPD and promote good practice.
c. Mandate CPD for their members and monitor compliance of registered individuals; and
d. Implement suitable sanctions for non-compliance of registered individuals.

Registered Professional Practitioners

All Licensed Bodies are expected to require that their members registered with the Council:

a. Display a commitment to CPD,
b. Plan and record their CPD in line with the competence requirements of their current organisation membership, qualification, and employment, and
c. Adhere to the Council's licensed body CPD policy and that of the Council.

Registrants who are temporarily not in active practice may request from their Licensed Body a temporary exemption from the requirements to submit a record of their CPD. It is for the membership body to agree any waiver of the CPD reporting requirement and the individual will therefore be exempt from an audit during this period. Upon return to "professional activity" the registrant will be subject to the normal CPD reporting requirements.

CPD CRITERIA FOR LICENSED BODIES

Any organisation licensed by the Council shall have a CPD policy and auditing process as outlined below that is compliant with the Council CPD Policy.

The Licenced Body policy shall:

- Mandate CPD recording, as described in the Council's Policy statement,
- Enable the registered professional to show continuous and ongoing development in terms of their discipline and career, demonstrating their ability to learn and reflect,
- Require the registered individual to record and reflect on their CPD as part of a continuous cycle of planned development.

In addition, licensed organisations are expected to support their members through the following:

- Encouraging a positive and proactive approach to CPD.
- Recommending a structured approach to CPD that registered individuals may use to plan and record their CPD appropriately, but which also allows flexibility for those who may be supported by an employer or other scheme.
- Support registered individuals by providing, or signposting them towards, guidance, resources, and support programmes, such as mentoring. These should be in line with current good practice, encouraging reflective practice to improve competence relevant to the registered individual's role and area of practice; and
- Providing effective feedback.

MONITORING OF CPD RECORDS FOR PROFESSIONALLY REGISTERED INDIVIDUALS

The Council's intention is to encourage a culture in which registered individuals will naturally engage in CPD and take ownership of their own learning and development. The Council believes that adopting this approach across the cyber security profession will help all registered individuals to plan and reflect on their own learning and development in a more conscious way, to their own benefit, to that of their employers, and of society.

Recording evidence of CPD undertaken is an important part of consciously planning and assimilating CPD and is therefore a requirement of professional registration.

A Licensed Body's policies must include appropriate processes to sanction registered individuals who persistently fail to comply with the Licensed Bodies CPD policy.

This should include the risk of removal from membership, and consequently the Council Register and therefore the ability to continue to use the Council's registration titles. The names of professionally registered individuals removed from the Register due to non-compliance with published CPD requirements will be made available to other Licensed Bodies as required.

GLOSSARY

Term	Definition
Accreditation	A quality assurance process recognising the minimum standards required for the quality of an educational curriculum.
Accredited	Award given to an entity (could be a programme, course, training scheme) that has been independently assessed as meeting the published requirements which may be expressed as learning outcomes, standards of competence or other). An accredited degree delivers some or all of the underpinning knowledge required as part of the overall competence and commitment standard that must be demonstrated for an individual to be awarded professional qualified status.
Applicant	(a) An organisation seeking admission as a Member of the UK Cyber Security Council or (b) an individual applying to a Licensed Body for assessment against the UK Cyber Security Council Standard(s) and admittance to the Register.
Approved (Qualification)	Recognition of the minimum standards required for a qualification.
Approved (Training Scheme/ Course)	Recognition of the minimum standards required for a training provider, including course content, instructors, and quality management systems.
Audit - internal	Internal audit: sometimes called a first-party audit, conducted by, or on behalf of, the organisation itself for internal purposes.
Audit - external	External audit: includes what are generally termed a 'second-' or 'third-party' audit. Second-party audits are conducted by parties having an interest in the organisation, such as customers, or by other persons on their behalf. Third-party audits are conducted by external independent organisations.
Career Pathway	The expectations, skills and development required for a professional specialism or area of practice along with details on progression through different roles.
Certified (training/qualification)	See Approved (Training Scheme/ Course).
Chartered	Status of an individual practitioner who has been assessed as meeting the standard for a Chartered qualification and been admitted to a register of Chartered professionals. In the context of the Council, those individuals who are on the (section of the) register as having achieved the Chartered Cyber Security Professional title.
Code of Conduct	A document adopted by an organisation as a means to regulate the behaviour of its constituent individuals with a focus on compliance and rules. Organisations that are Licensed Bodies of the Council will be required to have a Code of Conduct for their members that are Registrants.

Commitment	Required as part of demonstrating meet standard for registration. Council registrants will demonstrate personal and professional commitment to society, their profession and the environment, and specifically commit to; comply with codes (ethics/conduct), undertake CPD, work in a way that aligns with the principles of sustainable development, and actively engage in the profession.
Contextualised Standard	A CSC standard for any category of registrant that is tailored by a CSC member organisation for a particular CSC specialism, without weakening any of the required standard.
Competence	The proven or demonstrated individual capacity to use know-how, skills, qualifications or knowledge in order to meet the usual, and changing, occupational situations and requirements. It is part of the requirement that must be demonstrated to be admitted to the Council Register and maintaining competence is required of registered cyber security professionals (see CPD below).
Conflict of Interest	A set of circumstances that create a risk that professional judgement or actions regarding a primary interest will be unduly influenced by a secondary interest
Continuing Professional Development (CPD)	This is the systematic acquisition of knowledge and skills, and the development of personal qualities, to maintain and enhance professional competence. In the context of the Council: The activities undertake by a professional (individual practitioner) in undertaking continued and proactive development of their competence to maintain a current and relevant level of practice. The Council will set out the over-arching requirement for individuals to maintain competence, with the expectation that appropriate structures and more detailed requirements are set by the licensed member organisations, and that they monitor individual compliance.
CSQF Recognised and CSQF Endorsed	Terms currently adopted by W/S to describe qualifications captured in the Qualifications Framework and Career Framework respectively. (May not be finally adopted.)
Cyber Security	Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that may be used to protect the cyber environment, organisation and user's assets. Organisation and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information/data in the cyber

	environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and assets against relevant security risks in the cyber environment. (Definition adapted referring to ITU-T X. 1205)
CyBOK	Cyber Security Body of Knowledge: A comprehensive Body of Knowledge to inform and underpin education and professional training for the cyber security sector. https://www.cybok.org/
Discipline	A specific area of cyber security practice with its own discrete, definable body of knowledge. (See also Specialism.)
Diversity	The range of individual differences amongst a community, where each individual is recognised to be unique and the differences may be in terms of race, ethnicity, gender, sexual orientation, socio-economic status, age, disabilities, religious beliefs, political beliefs, or other ideologies.
Ethics Committee	A body comprising independent, impartial and multi-disciplinary individuals empowered to review the content of the UKCSC Codes of Ethics and/or Conduct and to consider cases where the consistent application of the duly established code(s) may not have been upheld and with the authority in such cases to apply documented sanctions where they are deemed appropriate.
Exemplifying Qualification	An educational or vocational qualification that demonstrates the knowledge, understanding and skills to meet or partly meet the Council's requirements for registration in a particular category. (See also Accreditation.)
Inclusion	A characteristic of a system or an organisation which describes its openness to a wide range of types of people. It has a relationship with diversity, in that the more inclusive an organisation is, the more diverse its members will tend to be.
Licensed Body	An incorporated body licensed by the Board (Council) to assess and nominate individuals for the appropriate register. Such organisations would be a 'Member' (to be defined) of the Council and use said licence to nominate individuals that are their individual members, hence providing the route for professional registration.
Member	A UK Cyber Security Council Member Organisation. The Council does not extend membership to individuals.
Peer Review	Evaluation of the reports, examinations, notes, data and findings by others competent in the same field to assess that there is an appropriate and sufficient basis for the opinions and/or conclusions
Practitioner	An individual providing a cyber security service at any level or stage as part of their work but is not necessarily doing so in a professional context.
Profession	An occupation with established standards. A profession can be a synonym for a career or trade but, in this context,

	it is a group identity for people who have skills relevant to a particular area of work. Most professions have other significant characteristics, most typically a structure which regulates entry into the profession and standards of practice.
Professional	(noun) A person who is a member of a profession OR (adjective) an attribute of a person or an organisational which describes their adherence to standards of behaviour which are typically expected of a member of a profession. A member of a professional organisation.
Professional Development	The combination of approaches, ideas and techniques that support individual learning and growth and by which an individual gains professional competence. It may take place through formal and informal learning, workplace training and experience, and voluntary activities.
Professionalism	A set of principles that inform good practice in the application of knowledge, skills and behaviours. In an individual, the characteristic of behaving professionally, generally taken to mean that an individual who exhibits professionalism puts the long-term interests of his/her profession and its positive role in society ahead of his/her own interests. A particular profession may require other qualities, such as possessing special knowledge, but these are not essential to professionalism.
Professional Registration	The process by which an individual is admitted to the UK Cyber Security Council Register.
Qualifications Directory	Term currently being used for the (on-line) listing of qualifications to be provided/facilitated by the Council (See also CSQF Recognised and CSQF Endorsed)
Qualifications Framework	A formal system of classifying qualifications and certifications for the purposes of quality assurance and comparability.
Recognised Standard	A UK Cyber Security Council standard which has been interpreted by a Council Licensed Body Member to reflect the particular characteristics of a particular cyber security specialism, whilst remaining compliant with the generic requirements.
The Register	Either (a) the list of UK Cyber Security Council Members (organisations) or (b) the list of individual cyber security professionals who have demonstrated the required standards of competence and commitment for a particular registration title.
Registration	Registration is the process of assessing and admitting (a) an organisation as a Council Member and (b) an individual to the Council Register of cyber security professionals.
Registrant	An individual cyber security professional who has demonstrated the Council's required standard of competence and commitment for one of the professional titles and been accepted onto the Register of professionals under that title.

Self-Regulatory Body	Professional self-regulation is a regulatory model which enables a level of voluntary control over the practice of a profession. Self-regulation is based on creating a body to regulate the activities of practitioners. In the UK, the agreement often takes the form of the Privy Council granting or recognising self-regulatory status through the award of a Royal Charter.
Regulation	A formal but non-statutory definition of mandatory behaviour in an activity which carries a risk of causing harm if it is not carried out correctly OR the exercise of oversight on an activity, a person or an organisation, or a group of any of these, to ensure that regulations are adhered to.
Revalidation	Generally used in reference to qualifications and fitness to practice. We are NOT proposing that the professional titles are revalidated, although registrants will need to undertake CPD to maintain competence.
Royal Charter	The legal entity type that shows an organisation is recognised and incorporated by Royal Charter.
Skills	In an individual - Proficiency, facility, or dexterity that is acquired or developed through training or experience. These include cognitive and technical aptitude, performance, practice, personal, interpersonal and behavioural abilities applied to the completion of tasks. (See also Competence) As defined by the National Cyber Security Skills Strategy: The combination of essential and advanced technical expertise and skills, strategic management skills, planning and organisation skills, and complementary soft skills that allow organisations to: Understand the current and potential future cyber risks they face Create and effectively spread awareness of cyber risks, good practice, and the rules or policies to be followed, upwards and downwards across the organisation Implement the technical controls and carry out the technical tasks required to protect the organisation, based on an accurate understanding of the level of threat they face Meet the organisation’s obligations with regards to cyber security, such as legal obligations around data protection Investigate and respond effectively to current and potential future cyber-attacks, in line with the requirements of the organisation.
Specialism	The principal field of professional activity, responsibility or practice.
Standards	The minimum standards of performance an individual must achieve when carrying out functions in the workplace, together with specifications of the underpinning knowledge and understanding.

The Cyber Security Profession (see also Cyber Security)	A vocation grounded in the principles outlined within the Cyber Security Body of Knowledge (CyBOK) and extensions as set out in the Scope of the Council requiring a level of expertise, experience, and high ethical standards from practitioners.
Professional Affiliate	An organisation that wishes to offer a route for professional registration to its (individual) members but is not currently licensed (and may not be able to achieve a license) can do so by becoming an Affiliate. This means they partner with a licensed organisation to complete the assessment process, with applicants being recommended to the Register through the Licensed Body partner. (Details on how this would be administered are yet to be defined.)