# STANDARD FOR PROFESSIONAL COMPETENCE & COMMITMENT (UK CSC SPCC)

VERSION 4.2

PUBLISHED OCTOBER 2024

UK CYBER SECURITY COUNCIL®

# TABLE OF CONTENTS

# ACKNOWLEDGEMENTS

The UK Cyber Security Council (the Council) acknowledges the cyber security guidance and support provided by the National Cyber Security Centre (NCSC) and the Department of Science, Information and Technology (DSIT) that has enabled a revision of the UKCSC Standard of Professional Competence & Commitment (UKCSC SPCC) to version 4.2.

The Council also acknowledges the collaborative input and support from its volunteer working groups, committees, and panels and from its collaborative partnerships with the following organisations:

- Chartered Institute of Information Security (CIISec)
- CREST
- ISACA
- ISC2
- SANS
- The British Computer Society (BCS)
- The Cyber Scheme
- The Institution of Engineering & Technology (IET)
- Members of the Council Strategic Advisory Panel (SAP)
- Members of the Council Specialism TAPs (Technical Advisory Panels)
- Members of the Council PSWG (Professional Standards Working Group)

# FOREWORD

Cyber security professionals operate across a wide range of areas within the cyber security profession. They respond to business and societal needs to prioritise the safety of individuals and employers from a cyber security perspective. Through the demonstration of professional competence and commitment to achieve professional registration, cyber security professionals highlight they are worthy of trust and operate ethically.

This document is the overarching Standard of Professional Competence and Commitment, known as the UK CSC Standard for Professional Competence and Commitment (UK CSC SPCC). It is used by the UK Cyber Security Council (the Council) to peer assess the competence and commitment of individuals working in cyber security roles, via its Licensed Bodies, to achieve professional registration. The Standard has been developed by cyber security professionals working across industry and academia.

Cyber security is a maturing profession, with a range of areas that require specialist insight, development, and practice. The UK CSC SPCC recognises the individual competence of a cyber security professional across a range of different Specialisms. The Council has contextualised a set of Specialisms from the Standard. These Specialisms provide a more specific and detailed definition of competence, against which professional registration may be recognised and awarded. The contextualised set of Specialisms are available to view via the Council's website: www.ukcybersecuritycouncil.org.uk.

# 1.UK CSC SPCC

## 1.1. Purpose

The primary purpose of the Standard is to describe the competence and commitment requirements that individuals must demonstrate to be professionally registered in each of the categories:

- Chartered Cyber Security Professional (ChCSP)
- Principal Cyber Security Professional (PriCSP)
- Practitioner Cyber Security Professional (PraCSP)
- Associate Cyber Security Professional (ACSP)

The Standard is aimed at different users, including:

- Individuals who are considering applying for professional registration. The Standard outlines the essential competences and professional commitments necessary to support a successful career in cyber security. Aspiring professionals can refer to this Standard as a roadmap to understand the expectations and requirements of the profession, helping them align their skills and aspirations with industry standards.

# 1.UK CSC SPCC

- Licensed Bodies, through which cyber security professionals become registered, play a crucial role in facilitating the registration process for cyber security professionals. The Standard equips the Licensed Bodies with a structured framework to evaluate and assess candidates seeking professional registration. By adhering to the guidelines outlined in the Standard, Licensed Bodies can ensure a rigorous assessment process, maintaining the integrity and credibility of the profession.

The Council, working collaboratively with industry representatives, contextualise the Standard for each Specialism, to bring the overarching UK CSC SPCC into context for each area of expertise within the profession, to ensure applicability. Different specialisms have unique standards, practices, and terminology; contextualisation helps ensure suitability for these requirements. It allows the Standard to remain overarching, accessible, and flexible. The contextualisation documents are available on the Council's website.

Contextualised standards are reviewed to ensure they are up to date and relevant to the sector at regular intervals.

# 1.UK CSC SPCC

This document includes the following:

- Professional Registration benefits
- Competence and commitment requirements
- Professional Registration process
- Revalidation requirements
- Continuing Professional Development (CPD) requirements

1.2. Regulations and Professional Registration Titles

The Council is the self-regulatory body for the UK's cyber security profession. It operates in accordance with the following regulations:

https://www.ukcybersecuritycouncil.org.uk/professional-standards-registration/professional-register/

# 1.UK CSC SPCC

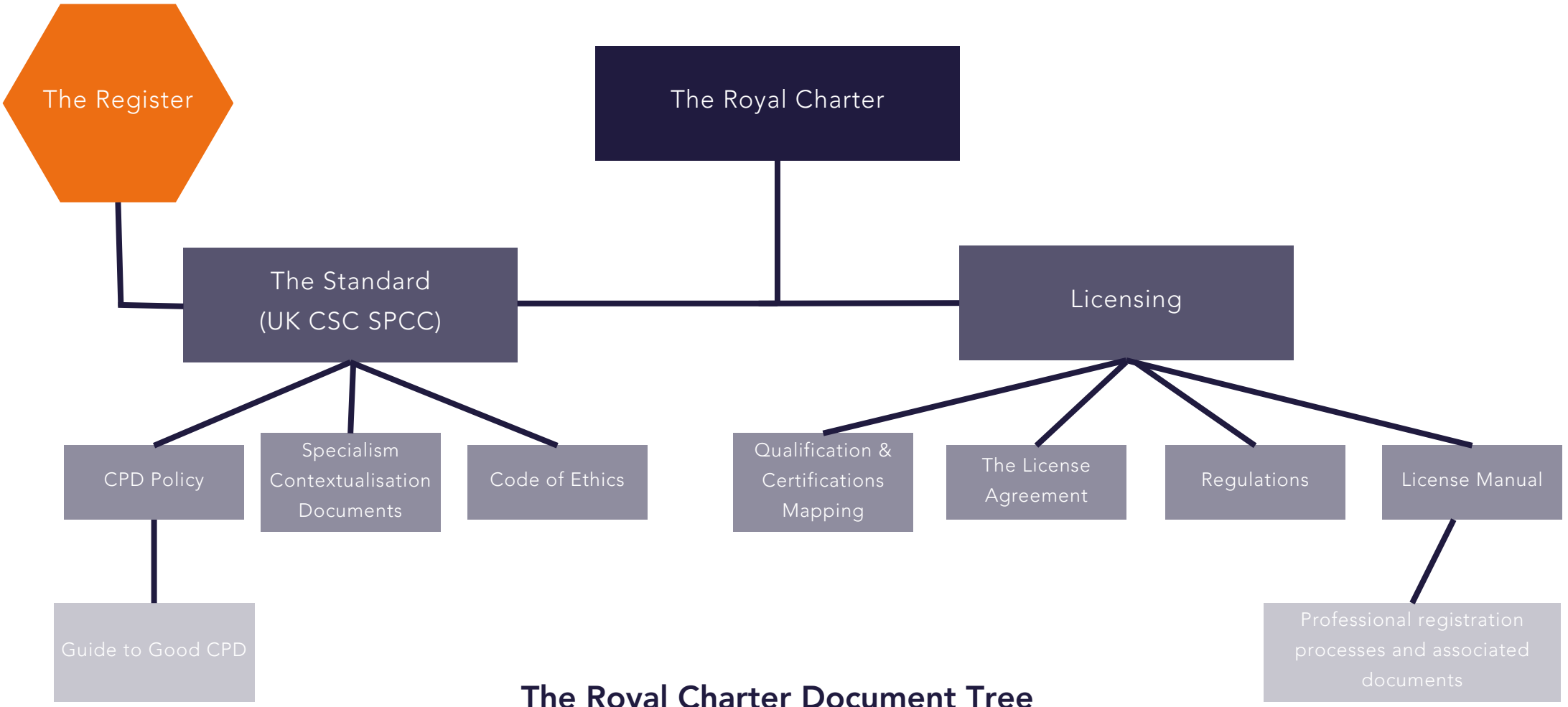
Under its Royal Charter, it sets industry standards and awards professional registration in four titles, which include post-nominals:

- Chartered Cyber Security Professional (ChCSP)
- Principal Cyber Security Professional (PriCSP)
- Practitioner Cyber Security Professional (PraCSP)
- Associate Cyber Security Professional (ACSP)

Each Professional Registration title has unique criteria for individuals to demonstrate their competence and commitment. While there is a progression between these professional registration titles, each one is also a noteworthy accomplishment in its own regard.

The UK Cyber Security Council Standard for Professional Competence and Commitment (UK CSC SPCC) referred to in this document as 'the Standard' or 'UK CSC SPCC must be viewed in the context of the the governance and operation of the Council as a royal charter body. You can see below a diagram of the governing and operational documents. You will find some of the documents in the diagram are available on the Council's website, which some documents are not available to the public.

# 1.UK CSC SPCC




**The Royal Charter Document Tree**

# 1.UK CSC SPCC

1.3. Licensed Bodies

The Council licenses organisations working with or within the cyber security sector, for specific Specialisms, and these organisations are known as Licensed Bodies.

Licensed Bodies play a crucial role in standardising the industry. They are experienced in their licensed Specialism and offer specialism-specific support to professionals and professionally registered individuals within the Specialism.

Licensed Bodies are licensed to assess the competence and commitment of individuals applying for the Council's professional registration titles via the registration process. To undertake the registration process, the Licensed Bodies appoint Assessors, who are required to be professionally registered. The Council provides training to all Assessors.

Licensed Bodies are subject to audit by the Council under the terms of their License Agreement, to ensure that the Standards are upheld, to maintain the integrity of the profession, and to maintain consistency and reliability in the industry.

# 2. PROFESSIONAL REGISTRATION: COMPETENCE, COMMITMENT AND BENEFITS

Professional registration provides assurance and recognition that an individual can meet the cyber security requirements of today, whilst also anticipating the needs of, and impact on, future generations. It demonstrates the individual has reached a set standard of knowledge, understanding and occupational competence. In addition, that the individual, following peer assessment, commits to developing and enhancing their knowledge and competence through active Continuing Professional Development (CPD).

Cyber security is a constantly changing and evolving profession with rapidly emerging technologies. It is essential, therefore, that professionally registered individuals demonstrate a commitment to maintaining their level of knowledge, understanding and skills in their chosen Specialism(s).

Professional registration provides employers, government, and society with confidence in the cyber security sector. It offers assurance of an individual's competence within the profession, as well as assurance of acting in a professional and ethical manner.

Individuals who continue to develop their knowledge, skills, and competence, throughout their cyber security career may progress between the professional registration categories, for example: Associate to Practitioner, Practitioner to Principal, and Principal to Chartered.

# 2. PROFESSIONAL REGISTRATION: COMPETENCE, COMMITMENT AND BENEFITS

## 2.1. Cyber Security competence for professional registration

Competence is defined as an individual's ability to conduct cyber security activities successfully. This includes possessing the underpinning knowledge, understanding and experience of wider cyber security.

For each professional registration title, the demonstration of competence and commitment is required in the following areas:

A - Knowledge, Understanding and Experience
B - Communication & Interpersonal Skills
C - Integrity
D - Professional Commitment
E - Collaborative Leadership & Mentoring

Underpinning knowledge and understanding is essential to competence, but it is not stand alone. Providing the technical expertise needed for a job, it forms the foundation of competence, gained through formal education, informal learning, training, or experience. This knowledge is crucial for meeting professional registration requirements and can be demonstrated through educational qualifications, certifications, work experience, or volunteering.

# 2. PROFESSIONAL REGISTRATION: COMPETENCE, COMMITMENT AND BENEFITS

2.2. Cyber Security commitment for professional registration

Cyber security professionals who apply for professional registration, via a Licensed Body, are required to demonstrate personal and professional commitment, demonstrate a set of values, and conduct that maintains their own reputation and that of the cyber security profession.

Cyber security is a constantly changing and evolving industry with rapidly emerging technologies. It is essential, therefore, that professionally registered individuals demonstrate a commitment to maintaining their level of knowledge, understanding and skills. Commitment can be demonstrated in a variety of ways, including Continued Professional Development, actively participating, and promoting cyber security, maintaining a working knowledge of technological advancements, compliance with appropriate legal and regulatory requirements, codes of conduct and ethics.

Professional ethics must be upheld. The Council has set the Standard and individuals who are professionally registered are responsible for ensuring that their day-to-day activities are of the highest ethical and moral standard.

# 2. PROFESSIONAL REGISTRATION: COMPETENCE, COMMITMENT AND BENEFITS

2.3. Benefits of professional registration

Professional registration provides various benefits to Registrants, their employers, and users of cyber security services. A full and updated list of benefits is available on our website here: https://www.ukcybersecuritycouncil.org.uk/professional-standards-registration/benefits-of-professional-registration/.

Registrants benefit from the recognition of their competence and commitment in cyber security, regardless of other certifications or education, thereby increasing credibility and employability. Their ethical standards are regulated by the Council and its Licensed Bodies, providing assurance to employers and clients. Professionals can tap into networks of other Cyber Security Professionals, through their Licensed Bodies and the Council, and have access to opportunities to give back to the profession.

Employers also benefit from the credibility of their staff and can demonstrate external validation of quality to clients. They can be assured their staff are peer reviewed as competent and ethical and they can structure staff development around the competences specific to the Professional Registration titles. They will be able to demonstrate eligibility for certain compliance schemes and provide assurance to clients working in sensitive sectors.

Users of cyber security services are best kept safe when they can be assured that competent, ethical professionals have developed or implemented their cyber security services and programmes.

# 3. PROFESSIONAL REGISTRATION PROCESS

The Professional registration process is a peer assessment model, which has been rigorously assessed to ensure that applicants who are awarded Professional Registration meet the requirements of the UK Cyber Security Council Standard of Professional Competence and Commitment Standard (UK CSC SPCC).

Peer assessment provides assurance that individuals are working to the Standard. Peers provide valuable insights into an individual's competence and performance, bringing diverse perspectives and experiences to the assessment process, offering a comprehensive evaluation of an individual. Peer assessment fosters a culture of continuous improvement, constructive feedback and support, which can help the industry and individuals to identify their strengths and weaknesses. It encourages professionals to support and learn from one another, fostering a culture of mutual respect and cooperation.

Peers are professionally registered individuals and trained by the Council to be formal Assessors. In most cases, assessors must be professionally registered in the same title as that to which the applicant is applying and have undertaken formal Assessor training provided by the Council.

# 3. PROFESSIONAL REGISTRATION PROCESS

3.1. Application, assessment and award

The Council is committed to offering choices that are diverse and inclusive. It provides a choice to applicants in terms of the assessment processes it offers for the competence assessment for professional registration. To achieve professional registration, applicants are peer assessed via one of the two registration processes:

- Process A (The three-stage peer assessment process)

This process has three stages, a documentary review of the written evidence, a professional discussion, and a final assessment.

- Process B (The two-stage, optional discussion, peer assessment process)

This process has two stages which comprise a documentary review of the written evidence and a final assessment. If further information is required, the Council, and by extension, the Licensed Bodies, reserve the right to invite an individual for a professional discussion (also referred to as an interview).

Both processes are documented in full on the Council's website.

# 3. PROFESSIONAL REGISTRATION PROCESS

3.2. Professional register of cyber security professionals

The Council owns and maintains a register of Cyber Security Professionals, referred to in this document as the Register.

Upon successful completion of the professional registration process, the Licensed Body will upload the Registrant details to the Register.

The Register holds the following details of each Registrant:

- Date and title of the professional registration award and Specialism (where relevant)
- Full name
- Any other information relevant to Specialism. For example, examination award for Security Testing

A Registrant will receive notification of their admittance to the Register and will receive a link they may use to share their entry on the Register with their employer or other person(s) of their choosing.

The Licensed Body and Council will not share details of the Registrant's entry on the Register with other persons or organisations without the Registrant's consent.

# 3. PROFESSIONAL REGISTRATION PROCESS

3.3. Professional registration revalidation

Registrants are required to revalidate their professional registration status annually to remain on the Council's Professional Register of Cyber Security Professionals and so retain the use of their professional registration post-nominals.

Registrants who fail to meet the requirements of the Standard will be removed from the Council's Professional Register of Cyber Security Professionals.

For Registrants to remain on the Council's Professional Register of Cyber Security Professionals, an annual fee must paid, by the Registrant, to the Licensed Body, which is then forwarded to the Council.

In addition, the Council requires Registrants to record 75 hours of CPD over 3 years which is submitted to the Licensed Body. The Council advises Registrants should record 25 hours of CPD annually for submission to their Licensed Body which contributes to the overall 75 hours across the three-year cycle.

Revalidation requirements (every three years):

- Payment of yearly fees to the Licensed Body, which are then forwarded to the Council.
- Relevant and approved CPD records to cover the required 75 hours over three years.

# 3. PROFESSIONAL REGISTRATION PROCESS

Once the above requirements are met, the revalidation date will be updated on the Council's Register of Cyber Security Professionals.

In the event where the revalidation process is not completed this will result in the automatic removal of the Registrant from the Register of Cyber Security Professionals.

A Registrant who fails to renew their professional registration with their Licensed Body may continue to hold their professional registration under these exceptional circumstances:

- The Licensed Body, with which the Registrant is professionally registered, has ceased to be a Licensed Body, or as an organisation has ceased to exist; or

- The relationship the Registrant held with the Licensed Body has lapsed or been cancelled, other than through being removed from the professional Register.

In such circumstances, the Registrant's professional registration status will remain valid, but only if, within twelve months of the cessation, the following requirements are met:

# 3. PROFESSIONAL REGISTRATION PROCESS

- The Registrant joins another Licensed Body and arranges for their professional registration status to be transferred to that Licensed Body with agreement from the Council and payment of the relevant fees. It is the responsibility of the Licensed Body to set any transfer fees.

- Once a Registrant has been informed that they are subject to disciplinary proceedings by the Licensed Body, through which they are registered, they may not transfer their professional registration status to another Licensed Body until the disciplinary process is complete.

Where a Registrant is suspended, the Licensed Body shall inform the Council. Any suspensions resulting from disciplinary action may be referred to the Council, if deemed appropriate by the Licensed Body.

# 3. PROFESSIONAL REGISTRATION PROCESS

## 3.4. Moving between Specialisms

Chartered, Principal and Practitioner Registrants will hold their professional registration against a chosen Specialism, which is often recognised as their deep specialist area of competence or their main specialist competence as a multi-disciplinary professional. The Associate professional registration title is not aligned to a Specialism.

The Council is reviewing how a Chartered, Principal and Practitioner Registrant may move between Specialisms. It is envisaged that once a formal process is confirmed, a Registrant will be able to move between Specialisms. The Council will publish further details relating to this on its website.

# 3. PROFESSIONAL REGISTRATION PROCESS

3.5. Disciplinary and appeal process

The disciplinary and appeal process relates only to applicants who are applying for professional registration and/or Registrants.

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 the right to an oral hearing and the right to representation. The Appeal Process is available to review on the Council's website.

An appeal will only be considered if all options with a Licensed Body have been exhausted. Appeals will be conducted in accordance with the process set out in the Licence Regulation.

A Registrant may be suspended from the Register while disciplinary or conduct allegations are investigated. This suspension may continue until the outcome of the disciplinary or conduct process outcome is confirmed.

# 4. CERTIFICATION FRAMEWORK

The Council has a certification framework to improve the navigability of the cyber security learning landscape.

Each of the Specialisms are built on the knowledge areas within the Cyber Body of Knowledge (CyBOK). The Council map certifications to the CyBOK knowledge areas, which indicates how certifications link to the Specialisms. The Council is continually mapping certifications using the certification framework.

The mapping work will extend further to identify where certifications, qualifications and training can be used to assure competence as part of the professional registration process.

The table, detailed below, provides alignment of the professional registration titles against varying education, competence, and skills frameworks. This provides reference to the expected level of knowledge, experience, skills, attitudes and behaviours for the professional registration titles that could be met through building underpinning knowledge and understanding.

# 4. CERTIFICATION FRAMEWORK

| Professional Registration Standard Requirements & Expected Equivalencies | Associate Cyber Security Professional (ASCP) Standard | Practitioner Cyber Security Professional (PraCSP) Standard | Principal Cyber Security Professional (PriCSP) Standard | Chartered Cyber Security Professional (ChCSP) Standard |
|---|---|---|---|---|
| Regulated Qualifications Framework (RQF) (1) and International Equivalency (2) | Level 3 | Level 3 | Level 6 | Level 7 |
| Credit and Qualifications Framework for Wales (CQFW) (3) | Level 3 | Level 3 | Level 6 | Level 7 |
| Scottish Credit and Qualifications Framework (SCQF) (4) | Level 6 | Level 6 | Level 10 | Level 11 |
| Skills Framework for the Information Age (5) | Level 1 | Level 3 | Level 5 | Level 6 |
| CIISec Skills Framework (6) | Level 2 | Level 3 | Level 5 | Level 6 |
| NICE Cybersecurity Workforce Framework (7) | Entry | Entry | Intermediate | Advanced |

(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

# 5. PROFESSIONAL REGISTRATION COMPETENCE AND COMMITMENT STATEMENTS - ASSOCIATE

5.1. Associate Cyber Security Professional (ACSP) 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 professional registration. They are intended as examples only, as the most appropriate evidence will vary with each individual. 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 experience which demonstrates their competence for the Associate Title and as such should be operating at a level at which they are either employed or ready to be employed within the cyber security profession.

# 5. PROFESSIONAL REGISTRATION COMPETENCE AND COMMITMENT STATEMENTS - ASSOCIATE

| Competence | The individual shall demonstrate that they: | Examples of Evidence<br>*should not be considered as complete or prescriptive and other types of evidence may be valid.* |
|---|---|---|
| **A - KNOWLEDGE, UNDERSTANDING & EXPERIENCE**<br><br>Associate Cyber Security Professionals will have demonstrated competence within areas of Cyber Security knowledge and are either employed in or ready for employment within Cyber Security. As such, they are operating at a level where their professional expertise could be used effectively in a cyber security role.<br><br>*This competence is about the knowledge and application of expertise within cyber security that allows for them to carry out a defined role effectively.* | **A-1. Can be engaged in a role or have practical experience of activities within Cyber Security.** | • Evidence of experience in either a simulated or real cyber security environment<br>• Current or recent employment within cyber security<br>• Completion of a professional certification alongside evidence of applied competence<br>• Completion of a cyber security apprenticeship<br>• Completion of an undergraduate or postgraduate cyber security degree<br>• Completion of an internship or Placement Year within cyber security<br>• Voluntary work that is cyber security related |
| | **A-2. Capable of problem solving to meet a customer / organisational cyber security requirement.** | • Evidence of experience in either a simulated or real cyber security environment<br>• Demonstration of problem-solving skills through employment or voluntary work<br>• Completion of a research project as part of an undergraduate or postgraduate degree |
| | **A-3. Capable of identifying opportunities for improvements to cyber security and contributing to solution development and implementation.** | • Involved in the implementation of an organisation's policy, processes and procedures, e.g. adherence to cyber security standards and controls<br>• Applied an improvement methodology to define and develop efficiencies across the organisation's cyber security operations<br>• Details of any voluntary or outreach work that supports an organisation's cyber security policies and processes<br>• A relevant dissertation or individual project within cyber security, including EPQ through to university level. |

# 5. PROFESSIONAL REGISTRATION COMPETENCE AND COMMITMENT STATEMENTS - ASSOCIATE

| Competence | The individual shall demonstrate that they: | Examples of Evidence<br>*should not be considered as complete or prescriptive and other types of evidence may be valid.* |
|---|---|---|
| **B - COMMUNICATIONS & INTERPERSONAL SKILLS**<br><br>Associate Cyber Security Professionals should demonstrate that they have reasonable communications and interpersonal skills.<br><br>*This competence is about being able to communicate and discuss aspects of cyber security with their peers and managers within an organisation.* | **B-1. Have good personal and social skills and awareness of diversity and inclusivity** | • Have good personal and social skills that demonstrate empathy, diversity and inclusivity |
| | **B-2. Have good oral and written communication skills.** | • Completion of a satisfactory application form<br>• Evidence of presentations or reports written as part of an accredited route to the professional register<br>• Evidence of explaining work to another person in a satisfactory and clear way either verbally or written |

# 5. PROFESSIONAL REGISTRATION COMPETENCE AND COMMITMENT STATEMENTS - ASSOCIATE

| Competence | The individual shall demonstrate that they: | Examples of Evidence<br>*should not be considered as complete or prescriptive and other types of evidence may be valid.* |
|---|---|---|
| **C - COLLABORATIVE MANAGEMENT, LEADERSHIP & MENTORING**<br><br>Associate Cyber Security Professionals should demonstrate that they understand the need to develop further skills and have carried out some supervised activity within either a real or simulated cyber security environment.<br><br>*This competence is about being able to operate in a cyber security environment.* | **C-1. Understand the responsibilities of operating in a cyber security environment.** | • Evidence of experience in a real or simulated cyber security environment<br>• Completion of a dissertation on a cyber security related subject<br>• Evidence of experience in a real or simulated cyber security environment<br>• Completion of a dissertation on a cyber security related subject<br>• Evidence of working as part of an apprenticeship<br>• Evidence of work experience, internship or voluntary work within cyber security<br>• Evidence of working in a cyber security role |
| | **C-2. Ability to be supervised and develop into a future cyber security practitioner.** | • Supervised cyber security training including responding to performance feedback<br>• Identified training requirements related to cyber security for self and others to implement a project or activity |
| | **C-3. Understand the need for organisational and time management skills.** | • Evidence of completion of a task or project that was time bounded<br>• Assisted in the organisation of a cyber security activity |
| | **C-4. Understand the need for a professional and secure working environment.** | • Carried out an activity in a real or simulated cyber security environment<br>• Studied the importance of policies and procedures as part of maintaining a secure environment |

# 5. PROFESSIONAL REGISTRATION COMPETENCE AND COMMITMENT STATEMENTS - ASSOCIATE

| Competence | The individual shall demonstrate that they: | Examples of Evidence<br>*should not be considered as complete or prescriptive and other types of evidence may be valid.* |
|---|---|---|
| **D - INTEGRITY**<br><br>Associate Cyber Security Professionals should demonstrate that they understand and apply integrity, morals, and ethical values.<br><br>*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.* | **D-1. Have personal and professional honesty and integrity.** | • Evidence of an example of personal ethics and integrity |
| | **D-2. Understand the need to comply with codes of conduct of professional organisations.** | • Either joined or committed to join a professional body when they are upon the register |
| | **D-3. Can understand and comply with appropriate legal and regulatory requirements.** | • Evidence that understanding of the importance of acting within the law<br>• Knowledge of legal and regulatory frameworks and suitable application<br>• Details of studying law-based modules at university or as part of apprenticeships or self-directed learning |

# 5. PROFESSIONAL REGISTRATION COMPETENCE AND COMMITMENT STATEMENTS - ASSOCIATE

| Competence | The individual shall demonstrate that they: | Examples of Evidence<br>*should not be considered as complete or prescriptive and other types of evidence may be valid.* |
|---|---|---|
| **E - PERSONAL COMMITMENT**<br><br>Associate Cyber Security Professionals should demonstrate that they carry out and plan for continued development of themselves and the cyber security profession.<br><br>*This competence is about demonstrating a commitment to continued development of their own knowledge and understanding for their 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.* | **E-1. Carry out and record Continuing Professional Development (CPD).** | • Provision of a plan for future CPD activities aligned to either changes in role or advancements in technology<br>• Provision of an apprenticeship log<br>• Provision of evidence of competency-based experience on a real or simulated cyber environment<br>• Details of any cyber security events that have been attended in the last 6 months<br>• Engaging in mentoring opportunities |
| | **E-2. Actively participate in the cyber security profession.** | • Commitment to Engagement in activities associated with the promotion of the cyber security profession<br>• Acting as an ambassador for Cyber Security at careers events |
| | **E-3. Maintain a working knowledge of technological advancements.** | • Demonstrating an interest in technology via a statement on the application form<br>• Engaging in sector webinars<br>• Self-directed learning<br>• Engaging with wider Cyber Security teams within workplace |

# 5. PROFESSIONAL REGISTRATION COMPETENCE AND COMMITMENT STATEMENTS - PRACTITIONER

5.2. Practitioner Cyber Security Professional (PraCSP) Standard

A Practitioner 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 Practitioner Cyber Security professional registration. They are intended as examples only, as the most appropriate evidence will vary with each individual role. The list should not be considered as complete or prescriptive and other types of evidence may be valid.

A Practitioner Cyber Security Professional will have practical experience in cyber security and be a practitioner operating at a level at which their professional expertise is being used effectively in their role.

# 5. PROFESSIONAL REGISTRATION COMPETENCE AND COMMITMENT STATEMENTS - PRACTITIONER

| Competence | The individual shall demonstrate that they: | Examples of Evidence<br>*should not be considered as complete or prescriptive and other types of evidence may be valid.* |
|---|---|---|
| **A - KNOWLEDGE, UNDERSTANDING & EXPERIENCE**<br><br>Practitioner Cyber Security Professionals should demonstrate their knowledge, understanding and experience relating to their specialism, some understanding of cyber security in its wider sense, and should be able to demonstrate practical experience within their career.<br><br>*This competence is about the knowledge and application of expertise within their career with some knowledge across the wider cyber security Specialisms that allows for them to carry out their role effectively.* | **A-1. Are engaging in a role or have practical experience of cyber security activities.** | • Involved in a cyber security issue and its rectification through the appropriate solution<br>• Involved in a cyber security incident with remediation, carrying out appropriate actions<br>• Involved in the analysis of a cyber security problem and production of recommendations from the results<br>• Involvement in the evaluating and documenting a requirements specification |
| | **A-2. Contributing to problem solving to meet a customer / organisational requirement.** | • Involved in a Cyber Security Operational Centre<br>• Involved in implementing a cyber resilience plan<br>• Involved in testing the cyber security environment |
| | **A-3. Have contributed to and engaged in continuous improvement to cyber security.** | • Contributed to evaluation and/or audit of an organisation's cyber security polices and processes and implemented improvements<br>• Applied an improvement methodology to define and implement efficiencies across the organisation's cyber security operations |

# 5. PROFESSIONAL REGISTRATION COMPETENCE AND COMMITMENT STATEMENTS - PRACTITIONER

| Competence | The individual shall demonstrate that they: | Examples of Evidence<br>*should not be considered as complete or prescriptive and other types of evidence may be valid.* |
|---|---|---|
| **B - COMMUNICATIONS & INTERPERSONAL SKILLS**<br><br>Practitioner Cyber Security Professionals should demonstrate that they have reasonable communications and interpersonal skills.<br><br>*This competence is about being able to communicate and discuss aspects of cyber security with their peers and managers within their organisation.* | **B-1. Have the ability to discuss cyber security effectively to both technical and non-technical audiences.** | • Any activity where they were involved in communicating the necessary information related to a cyber security assignment |
| | **B-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 |
| | **B-3. Have good oral and written communication skills.** | • Delivery of any report, paper, presentation, or other talk related to cyber security<br>• Other activities were communicating effectively with an audience was involved |

# 5. PROFESSIONAL REGISTRATION COMPETENCE AND COMMITMENT STATEMENTS - PRACTITIONER

| Competence | The individual shall demonstrate that they: | Examples of Evidence<br>*should not be considered as complete or prescriptive and other types of evidence may be valid.* |
|---|---|---|
| **C - COLLABORATIVE MANAGEMENT, LEADERSHIP & MENTORING**<br><br>Practitioner 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.<br><br>*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.* | **C-1. Understand the management of resources in a cyber security environment.** | • Supervised the delivery a minor cyber security project<br>• Supervised an activity within a cyber security project including effective communication with connected activities<br>• Supervised the delivery of a cyber security activity, working with external partners |
| | **C-2. Are able to supervise and develop people.** | • Supervised cyber security training including responding to performance feedback<br>• Identified training requirements related to cyber security for self and others in order to implement a project or activity |
| | **C-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<br>• Assisted in the organisation of a cyber security activity |
| | **C-4. Understand the need for a professional and secure working environment** | • Carried out cyber security activity where the security of the environment had to be maintained<br>• Involved in developing policies or procedures to ensure a professional environment was established or maintained |

# 5. PROFESSIONAL REGISTRATION COMPETENCE AND COMMITMENT STATEMENTS - PRACTITIONER

| Competence | The individual shall demonstrate that they: | Examples of Evidence<br>*should not be considered as complete or prescriptive and other types of evidence may be valid.* |
|---|---|---|
| **D - INTEGRITY**<br><br>Practitioner Cyber Security Professionals should demonstrate that they understand and apply integrity, morals, and ethical values.<br><br>*This competence is about demonstrating a core commitment to the cyber security profession.*<br><br>*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.*<br><br>*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.* | **D-1. Have personal and professional honesty and integrity.** | • Provide an example where their cyber security responsibilities were carried out in an ethical manner<br>• Provide an example where unethical behaviour / poor practice in others was challenged<br>• Where monitoring of their own performance produced an awareness of their own professional limitations<br>• Where privacy and ethical considerations were respected whilst performing their cyber security activities whilst adhering to organisation policies and objectives |
| | **D-2. Comply with codes of conduct of their professional membership organisation.** | • Any incident where confidential whistleblowing may have been carried out<br>• The identification of a code of conduct requirement that was particularly relevant to a cyber security incident or activity |
| | **D-3. Understand and comply 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 |
| | **D-4. Are able to identify and implement appropriate standards.** | • Any activity where conformance to standards related to a specific cyber security activity was carried out<br>• Any activity where non cyber security standards were implemented as part of a cyber security activity and how conformance was assessed |

# 5. PROFESSIONAL REGISTRATION COMPETENCE AND COMMITMENT STATEMENTS - PRACTITIONER

| Competence | The individual shall demonstrate that they: | Examples of Evidence<br>*should not be considered as complete or prescriptive and other types of evidence may be valid.* |
|---|---|---|
| **E - PERSONAL COMMITMENT**<br><br>Practitioner Cyber Security Professionals should demonstrate that they carry out and plan for continued development of themselves and the cyber security profession.<br><br>*This competence is about demonstrating a commitment to continued development of their own knowledge and understanding of cyber security; improving their knowledge and skills of the wider cyber security profession; and understanding and adapting to advances in technology and to the promotion of the profession.* | **E-1. Carry out and record Continuing Professional Development (CPD) or an acceptable equivalent.** | • 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 |
| | **E-2. Actively participate and promote the cyber security profession.** | • Engagement in activities associated with the promotion of the cyber security profession |
| | **E-3. Maintain a working knowledge of technological advancements.** | • Carrying out activities to identify advances related to cyber security |

# 5. PROFESSIONAL REGISTRATION COMPETENCE AND COMMITMENT STATEMENTS - PRINCIPAL

5.3. Principal Cyber Security Professional (PriCSP) 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 professional registration. They are intended as examples only as the most appropriate evidence will vary with each individual role and their associated 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 Specialism, at which they are an expert practitioner, and have experience in other Specialisms. As such, they should be operating at a level where their professional expertise may reasonably be sought to contribute to the development of their specific Specialism.

# 5. PROFESSIONAL REGISTRATION COMPETENCE AND COMMITMENT STATEMENTS - PRINCIPAL

| Competence | The individual shall demonstrate that they: | Examples of Evidence<br>*should not be considered as complete or prescriptive and other types of evidence may be valid.* |
|---|---|---|
| **A - KNOWLEDGE, UNDERSTANDING & EXPERIENCE**<br><br>Principal Cyber Security Professional should demonstrate their knowledge, understanding and experience relating to their Specialism, including experience of cyber security in another Specialism<br><br>*This competence is about the depth of knowledge and application of expertise within their own Specialism, with some knowledge and expertise across the wider cybersecurity Specialisms 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.* | **A-1. Are engaged in a role or have practical experience of activities that have a degree of complexity within their Specialism.** | • Managing the investigation of a cyber security issue, identifying workable solutions and selection of most appropriate solution<br>• Responded to a cyber security incident, assisted in identifying appropriate actions and subsequent implementation of a remediation plan<br>• Investigating a cyber security problem, carrying out analysis and recommending the results<br>• Leading the evaluating of a cyber security requirement and developing a requirements specification |
| | **A-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<br>• Involved in managing a Cyber Security Operational Centre for a customer / organisation<br>• Managed the implementation of a cyber resilience plan<br>• Involved in establishing a test and reference facility for a customer / organisational operational environment. |
| | **A-3. Have planned or delivered continuous improvement to cyber security.** | • Evaluated and/or audited an organisation's cyber security objectives and implemented improvements<br>• Applied an improvement methodology to define and implement efficiencies across the organisation's cyber security operations |

# 5. PROFESSIONAL REGISTRATION COMPETENCE AND COMMITMENT STATEMENTS - PRINCIPAL

| Competence | The individual shall demonstrate that they: | Examples of Evidence<br>*should not be considered as complete or prescriptive and other types of evidence may be valid.* |
|---|---|---|
| **B – COMMUNICATIONS & INTERPERSONAL SKILLS**<br><br>Principal Cyber Security Professionals should demonstrate that they have appropriate communications and interpersonal skills to fulfil their role within their organisation. This includes communicating with those who may have little or no knowledge of cyber security.<br><br>*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.* | **B-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 |
| | **B-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<br>• How a business requirement and priorities were translated into cyber security activities and actions<br>• The preparation of reports or specifications as part of a bidding process for a cyber security product or service |
| | **B-3. Have good personal and social skills that demonstrate empathy, diversity, and inclusivity.** | • Creating or enhancing a productive working relationship within an organisation or with a customer<br>• By taking a variety of perspectives and approaches to develop a collaborative cyber security solution<br>• Working within a team to develop collective cyber security goals with a challenging team dynamic<br>• Any activity that recognised equality, diversity, or inclusivity as a factor during a cyber security incident |
| | **B-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<br>• Contributed to a scientific cyber security paper or article utilising knowledge and expertise from the Specialism<br>• Presenting a cyber security remediation plan |

# 5. PROFESSIONAL REGISTRATION COMPETENCE AND COMMITMENT STATEMENTS - PRINCIPAL

| Competence | The individual shall demonstrate that they: | Examples of Evidence<br>*should not be considered as complete or prescriptive and other types of evidence may be valid.* |
|---|---|---|
| **C - COLLABORATIVE MANAGEMENT, LEADERSHIP & MENTORING**<br><br>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.<br><br>*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 Specialism.* | **C-1. Are able to manage resource, people, budgets in a cyber security environment.** | • Responsible for delivering cyber security activity demonstrating the management of associated risk<br>• Management of an organisational cyber security team especially during a cyber security incident<br>• Managing a cyber security project from requirements through to implementation<br>• Leading the execution and delivery of a cyber security project with external partners |
| | **C-2. Are able to lead, manage and develop people.** | • Managing cyber security teams and individuals with specialist training requirements<br>• Delivering effective cyber security training / education in their Specialism<br>• Managing a cyber security training team, monitoring the training provided, including performance feedback<br>• Led an ad-hoc team including non cyber security personnel in responding to a cyber security incident |
| | **C-3. Have good organisational and time management skills.** | • Established a new cyber security team within an organisation including measures to monitor effectiveness<br>• Managed cyber security activities in an effective way that improved the overall organisational security posture relative to the risk<br>• Managed the setting and delivery of cyber security activities to deadlines |
| | **C-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<br>• How a secure environment was established to manage a cyber security activity for a diverse set of individuals |

# 5. PROFESSIONAL REGISTRATION COMPETENCE AND COMMITMENT STATEMENTS - PRINCIPAL

| Competence | The individual shall demonstrate that they: | Examples of Evidence<br>*should not be considered as complete or prescriptive and other types of evidence may be valid.* |
|---|---|---|
| **D – INTEGRITY**<br><br>Principal Cyber Security Professionals should demonstrate that they have high levels of integrity, morals and ethical values.<br><br>*This competence is about demonstrating a core commitment to the cyber security profession.*<br>*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.*<br><br>*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.* | **D-1. Have personal and professional honesty and integrity.** | • Provide an example where their cyber security responsibilities were carried out in an ethical manner<br>• Provide examples where unethical behaviour / poor practice in others, was challenged<br>• Where monitoring of their own performance produced an awareness of their own professional limitations<br>• Where privacy and ethical considerations were respected whilst performing their cyber security activities whilst adhering to organisation policies and objectives<br>• Management of an issue where privacy and ethical issues gave rise to an impact on trust |
| | **D-2. Comply with codes of conduct of their professional membership organisation.** | • The escalation of 'prominent issues' discovered that may have included confidential whistleblowing<br>• The identification of specific aspects of the code that were particularly relevant to a cyber security incident or activity |
| | **D-3. Understand and comply with appropriate legal and regulatory requirements.** | • The identification of legal requirements within which they had to work, including how compliance was met<br>• Identification of non-UK legal & regulatory requirements during a cyber security activity<br>• Activities where legal frameworks covering transfers of personal data from UK to non-UK countries were identified and how compliance was achieved |
| | **D-4. Are able to identify and implement appropriate standards** | • Identification, implementation, and conformance to standards related a specific cyber security activity<br>• Identification of non cyber security standards that were implemented as part of a cyber security activity and how conformance was assessed |

# 5. PROFESSIONAL REGISTRATION COMPETENCE AND COMMITMENT STATEMENTS - PRINCIPAL

| Competence | The individual shall demonstrate that they: | Examples of Evidence<br>*should not be considered as complete or prescriptive and other types of evidence may be valid.* |
|---|---|---|
| **E - PERSONAL COMMITMENT**<br><br>Principal Cyber Security Professionals should demonstrate that they are committed to the continued development of themselves and the cybersecurity profession.<br><br>*This competence is about demonstrating a commitment to continued development of their own knowledge and understanding for their 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.* | **E-1. Carry out and record Continuing Professional Development (CPD) or an acceptable equivalent.** | • 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 |
| | **E-2. Actively participate and promote the cyber security profession.** | • Engagement in activities associated with the promotion of the cyber security profession<br>• Engagement in activities associated supporting charities and other organisations that do not have a cyber security capability<br>• Attendance at non cyber security events to promote the profession |
| | **E-3. Maintain a working knowledge of technological advancements and threat space.** | • Carrying out horizon scanning activities for future cyber security trends related to their / Specialism<br>• The management of a cyber security alerting function at the organisational level |

# 5. PROFESSIONAL REGISTRATION COMPETENCE AND COMMITMENT STATEMENTS - CHARTERED

5.4. Chartered Cyber Security Professional (ChCSP) 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 professional registration. They are intended as examples only as the most appropriate evidence will vary with each individual role and their associated 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 knowledge in several Specialisms, though should have a particular Specialism at which they are an acknowledged expert. As such, they 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.

# 5. PROFESSIONAL REGISTRATION COMPETENCE AND COMMITMENT STATEMENTS - CHARTERED

| Competence | The individual shall demonstrate that they: | Examples of Evidence<br>*should not be considered as complete or prescriptive and other types of evidence may be valid.* |
|---|---|---|
| **A - KNOWLEDGE, UNDERSTANDING & EXPERIENCE**<br><br>Chartered Cyber Security Professionals should demonstrate their knowledge, understanding and experience relating to their Specialism, including understanding of cyber security in its widest sense and should be able to demonstrate knowledge across a number of security Specialisms.<br><br>*This competence is about the depth of knowledge and application of expertise, not only within their own Specialism but across a number of related Specialisms that allows for the development of novel and unexpected solutions to address cyber security challenges.* | **A-1. Have led, managed, or carried out activities that have a degree of complexity within their Specialism or across a number of Specialisms 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<br>• Responding to a significant cyber security incident, identifying appropriate actions and implementation of a remediation plan<br>• Researching a complex cyber security problem, carrying out analysis and evaluating the results<br>• Evaluating a cyber security requirement, developing a requirements specification, analysing the market, selecting, and implementing the solution<br>• Secure the scene, capture, and process evidence in accordance with recognised practice and procedure to demonstrate repeatability in legal proceedings (E.g., ACPO guidelines) |
| | **A-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<br>• Evaluated new business operational requirements, developed, agreed, and implemented appropriate cyber security controls<br>• Evaluating and establishing a Cyber Security Operational Centre for a customer / organisation<br>• Development and establishment of a cyber resilience plan including consideration of people, processes, physical and technological requirements<br>• Researching, evaluating, and establishing a test and reference facility for a customer / organisational operational environment<br>• Development of a strategic cyber security plan from scratch for an organisation |
| | **A-3. Have led, managed, or coordinated continuous improvement to cyber security.** | • Evaluated and/or audited an organisation's cyber security strategy and implemented improvements<br>• Applied an improvement methodology to define and implement efficiencies across the organisation's cyber security operations |

# 5. PROFESSIONAL REGISTRATION COMPETENCE AND COMMITMENT STATEMENTS - CHARTERED

| Competence | The individual shall demonstrate that they: | Examples of Evidence<br>*should not be considered as complete or prescriptive and other types of evidence may be valid.* |
|---|---|---|
| **B - COMMUNICATIONS & INTERPERSONAL SKILLS**<br><br>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.<br><br>*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.* | **B-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 |
| | **B-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<br>• How a business requirement and priorities were translated into cyber security consequences and agreed mitigations<br>• The preparation of reports, drawings, budgets, and specifications etc. as part of a bidding process for a cyber security product or service |
| | **B-3. Have good personal and social skills that demonstrate empathy, diversity, and inclusivity.** | • Creating, maintaining, and enhancing productive working relationships within an organisation or with a customer including a degree of conflict resolution<br>• Demonstrating creativity by taking a variety of perspectives, taking account of unpredictable adversaries, threat behaviours and approaches and developing collaborative solutions<br>• Working with a team to develop collective cyber security goals during a changing interpersonal situation<br>• Provision of support during a cyber security incident, ensuring the needs of others were met, especially from a diversity and inclusion perspective |
| | **B-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<br>• Contributing to a published scientific cyber security paper or article as an author<br>• Presenting a published cyber security academic paper at an academic conference |

# 5. PROFESSIONAL REGISTRATION COMPETENCE AND COMMITMENT STATEMENTS - CHARTERED

| Competence | The individual shall demonstrate that they: | Examples of Evidence<br>*should not be considered as complete or prescriptive and other types of evidence may be valid.* |
|---|---|---|
| **C - COLLABORATIVE MANAGEMENT, LEADERSHIP & MENTORING**<br><br>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.<br><br>*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.* | **C-1. Are able to manage resource, people, budgets in complex and/or high- pressure cyber security environments.** | • Being accountable or having responsibility for delivering a complex cyber security activity with significant risk<br>• The successful management of an organisational cyber security team during a major incident<br>• The planning and budgeting of a cyber security project from concept through to commissioning<br>• The planning, execution, and delivery of a complex cyber security research project with external research partners<br>• Led teams conducting investigations using forensic techniques and tools. Experienced in using multiple forensic tools and techniques |
| | **C-2. Are 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<br>• Developing and delivering cyber security education at MSc level or in some other way exerting influence that contributes significantly to the field)<br>• 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<br>• Where human behaviours in the context of cyber risk and risk related decisions were identified and managed effectively |

# 5. PROFESSIONAL REGISTRATION COMPETENCE AND COMMITMENT STATEMENTS - CHARTERED

| Competence | The individual shall demonstrate that they: | Examples of Evidence<br>*should not be considered as complete or prescriptive and other types of evidence may be valid.* |
|---|---|---|
| **C - COLLABORATIVE MANAGEMENT, LEADERSHIP & MENTORING**<br><br>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.<br><br>*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.* | **C-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<br>• 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<br>• The consistent setting and meeting of deliverable deadlines in cyber security activities |
| | **C-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<br>• How a secure collaboration space was established to develop a cyber security solution for a diverse set of stakeholders |

# 5. PROFESSIONAL REGISTRATION COMPETENCE AND COMMITMENT STATEMENTS - CHARTERED

| Competence | The individual shall demonstrate that they: | Examples of Evidence<br>*should not be considered as complete or prescriptive and other types of evidence may be valid.* |
|---|---|---|
| **D - INTEGRITY**<br><br>Chartered Cyber Security Professionals should demonstrate that they have the highest level of integrity, morals, and ethical values.<br><br>*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.* | **D-1. Have personal and professional honesty and integrity.** | • Provide examples of carrying out their cyber security responsibilities in an ethical manner<br>• Provide examples where unethical behaviour / poor practice in others, especially where this might cause harm, was challenged and managed<br>• Where diligence in their own performance and advice produced an awareness of their professional limitations<br>• Identifying and respecting privacy and ethical considerations raised during their cyber security activities whilst adhering to organisation policies and objectives<br>• Where an awareness of privacy and ethics issues gave rise to an impact on trust and confidence and how this was managed |
| | **D-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<br>• Identifying specific aspects of the code that are particularly relevant to either the current or previous cyber security role |

# 5. PROFESSIONAL REGISTRATION COMPETENCE AND COMMITMENT STATEMENTS - CHARTERED

| Competence | The individual shall demonstrate that they: | Examples of Evidence<br>*should not be considered as complete or prescriptive and other types of evidence may be valid.* |
|---|---|---|
| **D - INTEGRITY**<br><br>Chartered Cyber Security Professionals should demonstrate that they have the highest level of integrity, morals, and ethical values.<br><br>*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.* | **D-3. Understand and comply with the appropriate legal and regulatory requirements.** | • Identification of legal parameters within which a cyber security professional had to work, that required compliance<br>• Identification of non-UK legal & regulatory requirements during a cyber security activity that required compliance<br>• Activities where legal frameworks covering transfers of personal data from UK to non-UK countries<br>• 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 |
| | **D-4. Are able to identify and implement appropriate standards.** | • Identification, implementation, and conformance to appropriate standards during a cyber security activity<br>• Identification of applicable non cyber security standards that were implemented as part of a cyber security activity |

# 5. PROFESSIONAL REGISTRATION COMPETENCE AND COMMITMENT STATEMENTS - CHARTERED

| Competence | The individual shall demonstrate that they: | Examples of Evidence<br>*should not be considered as complete or prescriptive and other types of evidence may be valid.* |
|---|---|---|
| **E - PERSONAL COMMITMENT**<br><br>Chartered Cyber Security Professionals should demonstrate that they are committed to the continued development of themselves and the cyber security profession.<br><br>*This competence is about demonstrating a commitment to continued development of their own knowledge and understanding for their Specialism; improving their knowledge and skills of the wider cyber security profession; and understanding and adapting to advances in technology and to the promotion of the profession.* | **E-1. Carry out and record Continuing Professional Development (CPD) or an acceptable equivalent.** | • 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 |
| | **E-2. Actively participate and promote the cyber security profession.** | • Engagement in activities associated with the promotion of the cyber security profession to schools<br>• Engagement in activities associated supporting charities and other organisations that do not have a cyber security capability<br>• Attendance at events that are not cyber security focussed where promotion through speaking or networking about cyber security was achieved |
| | **E-3. Maintain a working knowledge of technological advancements and threat space.** | • Carrying out horizon scanning activities for future cyber security trends<br>• The establishment and maintenance of a cyber security alerting function at either the organisational or personal level |

# 6. COMPARISON OF STANDARDS

| Associate | Practitioner | Principal | Chartered |
|---|---|---|---|
| An Associate Cyber Security Professional will have demonstrated competence in a number of cyber security areas of knowledge or in a specific Specialism at which they are either employed in or ready for employment as and as such should be operating at a level where their professional expertise is or could be used effectively in a cyber security role. | A Practitioner Cyber Security Professional will have practical experience in a specific 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. | A Principal Cyber Security Professional will have practical experience in a specific Specialism at which they are an expert practitioner and have experience in other 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 Specialism. | A Chartered Cyber Security Professional will have significant practical experience in several Specialisms, though may still have a particular 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. |

# 6. COMPARISON OF STANDARDS

| Associate | Practitioner | Principal | Chartered |
|---|---|---|---|
| Associate Cyber Security Professionals shall demonstrate:<br><br>• Their knowledge, understanding and experience relating to their understanding of cyber security in its wider sense and should be able to demonstrate evidence of competence either across the breadth of cyber security or within their Specialism.<br>• They have demonstratable communications and interpersonal skills.<br>• They understand the need to develop further skills and have carried out some supervised activity within either a real or simulated cyber security environment.<br>• They understand and apply integrity, morals, and ethical values.<br>• They carry out and plan for continued development of themselves and the cyber security profession. | Practitioner Cyber Security Professionals shall demonstrate:<br><br>• Their knowledge, understanding and experience relating to their Specialism including some understanding of cyber security in its wider sense and should be able to demonstrate practical experience within their Specialism.<br>• They have reasonable communications and interpersonal skills.<br>• They understand the need to develop management skills and have carried out some supervisory activity within a cyber security environment.<br>• They understand and apply integrity, morals, and ethical values.<br>• They carry out and plan for continued development of themselves and the cyber security profession. | Principal Cyber Security Professionals shall demonstrate:<br><br>• Their knowledge, understanding and experience relating to their / Specialism including experience of cyber security in another / Specialism.<br>• 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.<br>• 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.<br>• That they have high levels of integrity, morals, and ethical values.<br>• That they are committed to the continued development of themselves and the cyber security profession. | Chartered Cyber Security Professionals shall demonstrate:<br><br>• Their knowledge, understanding and experience relating to their Specialism including understanding of cyber security in its widest sense and should be able to demonstrate practical experience across a number of security Specialisms.<br>• 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.<br>• 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.<br>• They have the highest level of integrity, morals, and ethical values.<br><br>• They are committed to the continued development of themselves and the cyber security profession. |

# 6. COMPARISON OF STANDARDS

| A - Knowledge, Understanding & Experience | | | |
|---|---|---|---|
| **Associate** | **Practitioner** | **Principal** | **Chartered** |
| Associate Cyber Security Professionals shall use their knowledge, understanding and experience relating to their Specialism including some understanding of cyber security in its wider sense and should be able to demonstrate practical experience within their Specialism.<br><br>The individual shall demonstrate that they:<br><br>• Are capable of being engaged in a role or have practical experience of activities within Cyber Security or in their chosen Specialism.<br>• Are capable of problem solving to meet a customer / organisational requirement.<br>• Have contributed and implemented continuous improvement to cyber security. | Practitioner Cyber Security Professionals shall use their knowledge, understanding and experience relating to their Specialism including some understanding of cyber security in its wider sense and should be able to demonstrate practical experience within their Specialism.<br><br>The individual shall demonstrate that they:<br><br>• Are engaged in a role or have practical experience of activities within their Specialism.<br>• Have engaged in problem solving to meet a customer / organisational requirement.<br>• Have contributed and implemented continuous improvement to cyber security. | Principal Cyber Security Professionals should demonstrate their knowledge, understanding and experience relating to their / Specialism including experience of cyber security in other Specialisms.<br><br>The individual shall demonstrate that they:<br><br>• Are engaged in a role or have practical experience of activities that have a degree of complexity within their Specialism.<br>• Have applied problem solving tools and techniques in meeting customer / organisational requirements.<br>• Have planned or delivered continuous improvement to cyber security | Chartered Cyber Security Professionals should demonstrate their knowledge, understanding and experience relating to their Specialism including understanding of cyber security in its widest sense and should be able to demonstrate practical experience across a number of security Specialisms.<br><br>The individual shall demonstrate that they:<br><br>• Have led, managed, or carried out activities that are complex across a number of Specialisms.<br>• Have applied analytical problem solving in meeting customer / organisational requirements.<br>• Have led, managed, or coordinated continuous improvement to cyber security. |

# 6. COMPARISON OF STANDARDS

| B. Communications & Interpersonal Skills | | | |
|---|---|---|---|
| **Associate** | **Practitioner** | **Principal** | **Chartered** |
| Associate Cyber Security Professionals should demonstrate that they have reasonable communications and interpersonal skills.<br><br>The individual shall demonstrate that they:<br><br>• Have good personal and social skills and awareness of diversity and inclusivity.<br>• Have good oral and written communication skills. | Practitioner Cyber Security Professionals should demonstrate that they have reasonable communications and interpersonal skills.<br><br>The individual shall demonstrate that they:<br><br>• Have the ability to discuss cyber security effectively to both technical and non-technical audiences.<br>• Have good personal and social skills and awareness of diversity and inclusivity.<br>• 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.<br><br>The individual shall demonstrate that they:<br><br>• Have the ability to explain cyber security effectively to technical and non-technical audiences.<br>• Can explain cyber security advice and direction in a way that is clearly understood by the intended audience.<br>• Have good personal and social skills that demonstrate empathy, diversity, and inclusivity.<br>• 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.<br><br>The individual shall demonstrate that they:<br><br>• Have the ability to question and listen, summarise, and explain cyber security appropriately.<br>• Provide and explain cyber security advice, direction and/or expert opinion, in a way that can clearly be understood by the intended audience.<br>• Have good personal and social skills that demonstrate empathy, diversity, and inclusivity.<br>• Have excellent oral and written communication skills for both technical and non-technical audiences. |

# 6. COMPARISON OF STANDARDS

| C. Collaborative Management, Leadership & Mentoring | | | |
|---|---|---|---|
| **Associate** | **Practitioner** | **Principal** | **Chartered** |
| Associate Cyber Security Professionals should demonstrate that they understand the need to develop further skills and have carried out some supervised activity within either a real or simulated cyber security environment.<br><br>The individual shall demonstrate that they:<br><br>• Understand the responsibilities of operating in a cyber security environment.<br>• Ability to be supervised and develop into a future cyber security practitioner.<br>• Understand the need for organisational and time management skills.<br>• Able to identify and implement appropriate standards. | Practitioner 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.<br><br>The individual shall demonstrate that they:<br><br>• Understand the management of resources in a cyber security environment.<br>• Are able to supervise and develop people.<br>• Have an understanding of the need for organisational and time management skills.<br>• Are able to identify and implement appropriate standards. | 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.<br><br>The individual shall demonstrate that they:<br><br>• Are able to manage resource, people, budgets in a cyber security environment.<br>• Are able to lead, manage and develop people.<br>• Have good organisational and time management skills.<br>• Can maintain a professional and secure working environment. | 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.<br><br>The individual shall demonstrate that they:<br><br>• Are able to manage resource, people, budgets in complex and/or high-pressure cyber security environments.<br>• Are able to lead, manage and develop people through coaching and mentoring.<br>• Have excellent organisational and time management skills.<br>• Can maintain a productive, professional, and secure working environment. |

# 6. COMPARISON OF STANDARDS

| D. Integrity | | | |
|---|---|---|---|
| **Associate** | **Practitioner** | **Principal** | **Chartered** |
| Associate Cyber Security Professionals should demonstrate that they understand and apply integrity, morals, and ethical values.<br><br>The individual shall demonstrate that they:<br><br>• Have personal and professional honesty and integrity.<br>• Understand the need to comply with codes of conduct of their future professional membership organisation.<br>• Understand and comply with appropriate legal and regulatory requirements. | Practitioner Cyber Security Professionals should demonstrate that they understand and apply integrity, morals, and ethical values.<br><br>The individual shall demonstrate that they:<br><br>• Have personal and professional honesty and integrity.<br>• Comply with codes of conduct of their professional membership organisation.<br>• Understand and comply with appropriate legal and regulatory requirements.<br>• Are able to identify and implement appropriate standards. | Principal Cyber Security Professionals should demonstrate that they have high levels of integrity, morals, and ethical values.<br><br>The individual shall demonstrate that they:<br><br>• Have personal and professional honesty and integrity.<br>• Comply with codes of conduct of their professional membership organisation.<br>• Understand and comply with appropriate legal and regulatory requirements.<br>• Are able to identify and implement appropriate standards. | Chartered Cyber Security Professionals should demonstrate that they have the highest level of integrity, morals, and ethical values.<br><br>The individual shall demonstrate that they:<br><br>• Have personal and professional honesty and integrity.<br>• Comply with codes of conduct of their professional membership organisation.<br>• Understand and comply with the appropriate legal and regulatory requirements.<br>• Are able to identify and implement appropriate standards. |

# 6. COMPARISON OF STANDARDS

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

# 7. CONTINUING PROFESSIONAL DEVELOPMENT (CPD)

CPD is the ongoing process of learning and development that professionals engage in to maintain and enhance their knowledge, skills, and competence throughout their careers. CPD encompasses various activities such as attending courses, workshops, conferences, seminars, online learning, reading relevant literature, participating in professional discussions, and gaining practical experience.

CPD is an integral part of professional registration and maintaining an individual's registration status. It enables professionals to stay up to date with the latest technology, developments, and advancements in cyber security. It may contribute to career progression and potential progression through recognition of the professional registration titles.

Learning through CPD should be reflective and should, where possible, relate to specific objectives. 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 their outcomes is a valuable process for turning learning into competence.

# 7. CONTINUING PROFESSIONAL DEVELOPMENT (CPD)

## 7.1. CPD Policy

CPD is a mandatory requirement for Registrants who are included on the Professional Register of Cyber Security Professionals, held by the UK Cyber Security Council. CPD is an integral and mandatory part of the competence requirements for all cyber security practitioners irrespective of role or Specialism.

CPD records are audited by the Licensed Bodies.

The Council advises that Registrants undertake and record 25 hours of CPD annually which contributes to the mandatory requirement of 75 hours of CPD over a three-year cycle and across several sources. The Council supports a culture where Registrants engage and record their CPD routinely and take ownership of their own learning and development.

A Registrant is required to comply with the Council's CPD Policy to maintain Registration. The CPD Policy and Guide to Good CPD can be found on the Council's website.

# 7. CONTINUING PROFESSIONAL DEVELOPMENT (CPD)

7.2. CPD Policy for Licensed Bodies

Licensed Bodies are required to hold a CPD policy and auditing process, as outlined below, which is compliant with the Council's CPD policy.

A Licensed Body's CPD policy shall:

- Require the Registrant to record and reflect on their CPD as part of a continuous cycle of planned development.

A Licensed Body supports their Registrants by:

- Encouraging a positive and proactive approach to CPD.
- Recommending a structured approach to CPD that Registrants may use to plan and record their CPD appropriately, and that also enables flexibility for Registrants who may be supported by an employer or via other scheme(s).
- Supporting Registrants by providing, or signposting them towards, guidance, resources, and support programmes, such as mentoring. These should be aligned to current best practice, encouraging reflective practice to improve competence relevant to the registered individual's role and area of practice.
- Providing effective feedback to the Registrant.

# 8. GLOSSARY

| Term | Definition |
|---|---|
| Applicant | (a) An organisation seeking admission as a Member of the UK Cyber Security Council or (b) an individual applying to a Licensee 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' audits. 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. |

# 8. GLOSSARY

| Term | Definition |
|---|---|
| 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 Licensees of the Council will be required to have a Code of Conduct for their members that are Registrants. |

# 8. GLOSSARY

| Term | Definition |
|---|---|
| Commitment | Required as part of demonstrating standard for registration are met. 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. |
| 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.<br><br>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<br>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. |

# 8. GLOSSARY

| Term | Definition |
|---|---|
| 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.<br>In the context of the Council: the activities undertaken by a professional (individual practitioner) in undertaking continued and proactive developmentof their competence to maintain a current and relevant level of practice.<br>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. |
| Cyber Security | Cyber security 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.<br>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. Cyber security strives to ensure the attainment and maintenance of the security properties of<br>the organisation and assets against relevant security risks in the cyber environment. (Definition adapted referring to ITU-T X. 1205). |

# 8. GLOSSARY

| Term | Definition |
|---|---|
| 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 UK CSC 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. |

# 8. GLOSSARY

| Term | Definition |
|---|---|
| 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. |
| Licensee / 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. |

# 8. GLOSSARY

| Term | Definition |
|---|---|
| Practitioner | 1) 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.<br>2) Practitioner is also a professional registration title. |
| 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.<br>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. |

# 8. GLOSSARY

| Term | Definition |
|---|---|
| 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. |
| Recognised Standard | A UK Cyber Security Council standard which has been interpreted by a Council Licensee 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. |

# 8. GLOSSARY

| Term | Definition |
|---|---|
| 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. |
| Royal Charter | The legal entity type that shows an organisation is recognised and incorporated by Royal Charter. |

# 8. GLOSSARY

| Term | Definition |
|---|---|
| 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.)<br><br>As defined by the National Cyber Security Skills Strategy: [EE1] 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:<br><br>• Understand the current and potential future cyber risks they face<br>• Create and effectively spread awareness of cyber risks, good practice, and the rules or policies to be followed, upwards and downwards across the organisation<br>• 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<br>• Meet the organisation's obligations with regards to cyber security, such as legal obligations around data protection<br>• 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. |

# 8. GLOSSARY

| Term | Definition |
| --- | --- |
| 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. |