

Associate Cyber Security Professional

Application Guidance Document



The Associate Cyber Security Professional title is the UK Cyber Security Council's entry-level Professional Title. It is designed for those at the start of their careers in cyber security. An Associate Cyber Security Professional will have demonstrated competence within key areas of cyber security knowledge and is either employed in an early career cyber role, or ready for their first role in cyber security.

Becoming an Associate Cyber Security Professional allows individuals to join the UK's Cyber Security Professional Register. They will become a registered cyber security professional and will be able to use the post-nominals ACSP.

This document provides guidance on your application to become an Associate Cyber Security Professional. You can find out more about the title and access the application form at ukcybersecuritycouncil.org/associate.

How you will be assessed:

Individuals applying for the Associate Cyber Security Professional title are assessed against the UK Cyber Security Council's Standard for Professional Competence and Commitment (the Standard). This government-backed, unified standard sets out clear criteria and competencies that demonstrate technical knowledge, leadership and ethics across each of our four professional titles.

[You can find the full Standard here.](#) Pages 25-29 cover the Associate title. We strongly recommend you carefully read this section of the Standard as it includes the questions you will be asked, and examples of the evidence you could provide to demonstrate you meet the required competencies. Please note that the examples of evidence given should not be considered complete or prescriptive.

When applying for your professional title, you will need to provide evidence that demonstrates your individual competence in **the following five competencies**:

A) Knowledge, Understanding and Experience

This competency demonstrates your cyber security knowledge, and your experience applying that knowledge in a cyber security setting. You should be able to demonstrate knowledge within key areas of cyber security, and either be employed in an early career role, or ready for employment in the cyber security sector.

B) Communication and Interpersonal Skills

This competency is about being able to communicate and discuss aspects of cyber security with peers and managers within an organisation. You should be able to demonstrate that you have reasonable communication and interpersonal skills.

C) Collaborative Management, Leadership and Mentoring

This competency is about being able to operate in a professional cyber security environment. You should be able to demonstrate that you have carried out some supervised activity within either a real or simulated cyber security environment, and understand the need to develop further skills.

D) Integrity

This competency is about demonstrating a core commitment to the cyber security profession, and understanding the importance of complying with codes of ethics, adherence to standards and with legal and regulatory requirements. You should be able to demonstrate that you can understand and apply integrity, morals and ethical values across your work.

E) Personal Commitment

This competency is about demonstrating a commitment to continued development of knowledge and understanding as well as adapting to advances in technology and the evolving cyber security landscape. You should be able to demonstrate that you carry out and plan for continued professional development.

Fast-Track Applications

To support you in your application, we have aligned a number of existing qualifications, certifications and training courses to the competencies required for the Associate title.

You do not need to hold any of these to be awarded an Associate title but, if you do, you may be able to fast-track your application. **Some of these routes fully align with the title**, meaning you have already shown you meet all the required competencies and don't have to provide us with that information again. **Others partially align**, meaning that you will automatically meet some of the competencies but will have to provide evidence for other areas as part of your application.

You can find a full list of these aligned routes at ukcybersecuritycouncil.org/associate.

Structuring Your Answers

Some tips for how to structure your answers when providing evidence for the required competencies:

- **We recommend that you structure your answers using an approach such as the STAR technique** as an effective way of demonstrating the application of your skill and knowledge to the competencies. This is a method of answering questions that is comprised of four steps:
 - **Situation:** Describe the situation and when it took place.
 - **Task:** Explain the task and what your goal was.
 - **Action:** Provide details about the action you took to attain this.
 - **Result:** Conclude with the results of your actions.
- **We recommend that you write using the first person.** Using "I" helps to make it clear what role you had in a situation, particularly if you are using an example where you worked in a team.
- **Try to avoid using acronyms** - if you do use them, make sure to explain them in full the first time you use them.
- **If your work is sensitive or you are concerned about Non-Disclosure Agreements** you have signed, please be aware that you don't need to name the institution or technology you are using, you can focus on the skills you used.

- **You may find yourself repeating evidence throughout your application and this is common in the application process.** You could try and describe different elements of a situation. The full application will be looked at by each assessor so you do not need to detail the same situation multiple times; you can refer to a previous point or highlight other relevant skills you utilised in the same situation.
- **You may find you need to draw on evidence from situations outside of cyber security,** especially if you are just starting out in the sector. This is fine but try to use cyber security examples where you can.

The Application Form

The application form is comprised of several sections:

- 1) Personal Information:** standard information including contact details and whether you require any reasonable adjustments to your application process.
- 2) Aligned Qualifications:** as mentioned above, if you have attained any of our aligned qualifications or certifications, you may be able to fast-track your application. In this section, you can let us know which of these, if any, you have attained.
- 3) Evidence of Competencies:** this is the main focus of the application form. In this section you can give evidence for each of the competencies mentioned above. Please note that the questions you are required to answer may change depending on what you have selected in the 'Aligned Qualifications' section. For example:
 - **If you have attained a fully aligned qualification,** you will be able to skip this section entirely, as you have already demonstrated you meet all the required competencies.
 - **If you have attained a partially aligned qualification,** you will be asked to provide evidence for some, but not all, of the competencies.
 - **And if you have not selected an aligned qualification,** that's fine, we'll lay out all the competency questions for you to answer in this section.
- 4) Attestor Details:** Unless you have achieved a fully aligned qualification or certification (in which case you do not require attestation), you will need to provide details of an attestor to confirm to us that they believe you meet the required competencies. [You can find more details about this in the appendix below.](#)
- 5) Declaration:** your agreement with the required terms of applying for a professional title.
- 6) Payment:** applications cost £99 +VAT and you can pay through our secure payment portal.

Accessibility Needs

You will have the opportunity to ask for reasonable adjustments to the assessment process in the application form. [You can find out more information about our approach to adjustments here.](#) If you have any accessibility needs that should be taken into consideration before this stage, please contact us via professionalisation@ukcybersecuritycouncil.org.uk.

Use of Artificial Intelligence (AI) in the Application Process

We understand that AI may improve accessibility for applicants such as those facing language barriers or disabilities, however, applicants must still demonstrate the knowledge and expertise needed to meet the necessary requirements for a professional title.

Applicants must adhere to the following guidelines regarding the use of AI in their evidence submitted to achieve a UK Cyber Security Council Professional Title. These guidelines include, but are not limited to, authenticity, accountability and ethical use.

- Applications must be based on the applicant's real skills, competences and experiences.
- AI may be used as a tool to refine answers, not create or mislead.
- Applicants accept full responsibility for the accuracy of their evidence submission.
- AI usage must align with ethical guidelines, ensuring that no intellectual property is compromised, and that the content is truthful and reflective of the applicant's professional and personal profile.

Ready to Apply?

If you have read all the information above, as well as [the Associate section on pages 25-29 of the UK Cyber Security Standard of Competence and Commitment](#), you're ready to apply.

You can access the application form at ukcybersecuritycouncil.org/associate.

Please note: The overall application timeline from submitting your application to receiving your outcome is about three months. Most applicants who submitted their application in the first half of this current application window (before 17th May) will hear their outcome by 02nd July. Most applicants who submit their application in the second half of this application window (between 17th May and 19th July) will hear their outcome by 25th September.

Appendix – Attestor Requirements

Depending on your application route, you may have to provide details for an attestor who will confirm to us that they believe you meet the required competencies for your professional title.

If you are completing a fast-tracked application with a fully aligned qualification or certification you will *not* require an attestor as part of your application.

If you are completing a fast-tracked application with a partially aligned qualification or certification that covers the A competencies only your attestor only needs to confirm your B-E competencies and only needs to be from List A below. They do not necessarily need to be a cyber security professional.

If you are completing a fast-tracked application with a partially aligned qualification or certification that covers the B-E competencies only your attestor will need to be able to confirm both your A and B-E competencies. You will need an attestor that meets one of the criteria from both Lists A and B below.

If you are completing a full application, without an aligned qualification or certification, your attestor will need to be able to confirm your A – E competencies. You will need an attestor that meets one of the criteria from both Lists A and B below.

If you require an attestor from both lists A and B, this can be the same person. For example, a registered cyber security professional can be your attestor for both lists. Please note that as part of the attestation process, your attestor will be able to view your application materials.

List A: an attestor who is a position of trust. For example:

- A Registered (Associate/Practitioner/Principal/Chartered) Cyber Security Professional
- Member of a UK Cyber Security Council Technical Advisory Panel
- Member of a UK Cyber Security Council Specialism Working Group
- Member of CII Sec.
- Member of ISC2
- Trustee of the UK Cyber Security Council
- Civil servant
- Armed forces member
- Police officer
- Teaching or research faculty at an accredited UK university
- Chartered in any discipline
- Member of a Royal Charter professional body
- Member of a regulated profession
- Magistrate
- An elected official in local, devolved, or national government
- A recipient of an honour (e.g. CBE; Damehood)

List B: an attestor who can speak to your cyber security competencies. For example:

- A Registered (Associate/Practitioner/Principal/Chartered) Cyber Security Professional.
- Member of a UK Cyber Security Council Technical Advisory Panel.
- Member of a UK Cyber Security Council Specialism Working Group.
- Member of CII Sec.
- Member of ISC2.
- Someone with a university degree in cyber security.
- Someone working in a cyber security role.
- Someone with a recent cyber security certification at RQF Level 3 or above.
- Someone who has published peer reviewed research in a cyber security topic.
- A lecturer or professor of cyber security.

Exclusions and Conflicts of Interest

An attestor must not have a major conflict of interest, such as being:

- A family member of the applicant, including by marriage e.g. step-parent.
- A current or former carer or guardian of the applicant.
- The applicant's spouse, partner, or any other individual with whom they have had, or currently have, a close personal relationship.
- The other parent of a child of the applicant.

- Someone who lives at the same address as the applicant.
- Someone who is supervised by the applicant in a professional, academic, or training setting.

What makes a good attestor:

The most effective attestors will:

- Be familiar with you professionally or academically.
- Be more experienced than you.
- Have supervised you at some point – though not necessarily as a line manager.
- Be familiar with the UK Cyber Security Council standard specifically or the principles of professional registration generally.

Some examples of good attestor roles/relationships include:

- Your university personal tutor, dissertation supervisor, or PhD supervisor.
- Your direct line manager.
- A trainer or teacher on a long programme.
- A senior colleague with whom you work closely.
- A mentor.

If you are unable to find an attestor that meets the criteria, please contact professionalisation@ukcybersecuritycouncil.org.uk.
