UK CYBER SECURITY COUNCIL®

Standard of Professional Competence and Commitment:

Cyber Security Governance and Risk Management

T

Contents

ACRONYM LIST

Council	UK Cyber Security Council
ChCSP	Chartered Cyber Security Professional
PCSP	Principal Cyber Security Professional
ACSP	Associate Cyber Security Professional
UKCSC SPCC	UK Cyber Security Council Standard of Professional Competence and Commitment
Assessor	A Council approved, trained and professional registered individual
Competences	Requirements listed in the UKCSC SPCC

Introduction:

The UK Cyber Security Council (Council) is a Royal Chartered organisation, setting industry standards and awarding professional titles for those working in the cyber security profession. The Council is responsible for holding the register of the UK's first Chartered Cyber Professionals.

The Council's mission is that the UK becomes the safest place in the world to work and live online. As part of this, it is important that the Council creates a vibrant and diverse cyber security professional, capable of cultivating the skills needed to ensure the UK is a world leader in cyber security.

The UKCSC SPCC is an overarching Standard and the Council, with support from industry, is creating contextualisation across 16 industry areas to support professional registration. They are referred to as specialisms. More information is available on the Council's website https://www.ukcybersecuritycouncil.org.uk/

This document has been created with the support of organisations such as Chartered Institute of Information Security (CIISec) and ISACA, to contextualise the overarching Standard, showing the typical types of working evidence you can provide to meet the competence and commitment statements for the professional titles listed in the UKCSC SPCC.

Assessment

In line with other specialisms, of the competences described via the UKCSC SPCC, the candidate will be expected to demonstrate a thorough and detailed knowledge of at least 80% whilst the remaining 20% will be demonstrated at, at least, an acceptable but lower level of understanding.

Contextualisation

The below table provides a comparison of the types of evidence and level of competence an individual may demonstrate for the two professional titles, Chartered Cyber Security Professional and Principal Cyber Security Professional.

The Chartered guidance below is building on the guidance described for the Principal category, it expands the level and depth of competence expected to be demonstrated by someone aligning with the Chartered category of professional registration.

This should not be viewed as a checklist but as a guide to the areas where knowledge will be expected and where various specialist areas of knowledge can be demonstrated. The interviewers will be using this guide as the basis for their questioning and challenging to assess the level of knowledge and understanding in each area.

Principal	Chartered
The ability to elicit security requirements, based on straight-forward analysis, that support the overall business need and the ability to map directly between security requirements and business needs.	The ability to elicit complicated, non-obvious security requirements that are directed by the overall business need, together with the direct mapping between business need, technology that supports that need, and how it might be impacted which may be non-trivial to deduce.
The ability to explain clearly how to determine applicable business assets / things of value and the impact on these assets should they be affected or compromised. This process, undertaken in conjunction with key stakeholders including a security architect, together with evidence from the use of some techniques, should arrive at an understanding of the security need. It could use techniques such as threat tree analysis, or the use of security principles-based derivation, or other more formal techniques such as from engineering.	The ability to explain clearly how to determine applicable business assets / things of value and the impact on these assets should they be affected or compromised. This process, undertaken in conjunction with key stakeholders including a security architect, together with evidence from the use of some techniques, should arrive at an understanding of the security need. It could use techniques such as threat tree analysis, or the use of security principles-based derivation, or other more formal techniques such as from engineering.
Recognises the limitations of risk analysis, for example for the determination of threat motivation, reputational impact, or complex system dynamics. Recognises the benefits of presenting alternative scenarios that elicit alternative risk dynamics.	Recognises the limitations of risk analysis, for example for the determination of threat motivation, reputational impact, or complex system dynamics. Recognises, and can explain in detail, the benefits of presenting alternative scenarios that elicit alternative risk dynamics.

Principal	Chartered
Able to explain and justify the approach to prioritisation of risks by comparing and balancing different types of risk from across the organisation.	Has a full knowledge of the regulations, standards, and legislation applicable to their organisation, and to the wider community in the UK.
Has a detailed technical knowledge of many / most of the latest types of tactical and operational risk treatment options.	Has the knowledge to make the key decisions on the choice of operational risk controls and capabilities in order to deliver the most effective security treatments meeting the competing business requirements.
Can help to determine the level of risk appetite and risk tolerance acceptable to an organisation.	Is able to ensure the methods used for risk analysis across the organisation are the most appropriate and effective with all options considered.
Can explain the detail of defense-in-depth and defense-in-breadth implementations, and how they are utilised in straight-forward and less complex situations.	Can explain the detail of defense-in-depth and defense-in-breadth implementations, and how they are utilised in complex, high-risk and / or high-impact situations.
Has a good and thorough knowledge of many of the regulations, standards, and legislation applicable to cyber-security in the UK, and specifically of those applicable within their own business environment. They should also have a good knowledge of the technical issues that the implementation of regulations, standards and legislation demand in order for their organisation to be compliant as applicable.	Has a deep and detailed knowledge of most of the regulations, standards, and legislation applicable to cyber-security in the UK and specifically of those applicable within their own business environment. They should also have a detailed knowledge of the technical issues that the implementation of regulations, standards and legislation demand in order for their organisation to be compliant as applicable.
Understands and communicates industry developments, and the role and impact of technology on cyber security.	Understands, and can communicate to a wider non-technical audience, industry developments, and the role and impact of technology on cyber security.

Whilst Associate is not linked to a specialism, here is some contextual guidance that details possible examples for applicants that have been involved in roles that are related to Cyber Security Audit and Assurance.

Associate
Can explain the basic principles of Information Security Governance and how it applies within an organisation together with some techniques to gain an understanding of an organisation's security needs.
Can explain the principal concepts and purposes of Information Security policies and standards.

Associate

Can explain the principles and practice of the risk management process such as:

1. establishing business need.
2. establishing the security direction and governance.
3. the approach to risk assessment.
4. the approach to treatment.
5. the assurance approaches.

Can explain the principles of risk management analysis and its appropriate and inappropriate use. Can demonstrate use of one or more methods of risk analysis, to determine those risks, most applicable and consistent with the contextual requirements.

Can explain the use, applicability, benefits, and limitations of qualitative versus quantitative risk analysis and of the definition and use of the terms risk appetite and risk tolerance.

Can explain the basic concepts of strategic risk treatments (treat, transfer, accept, etc.) and how they can be implemented in straight-forward situations / systems together with the principles of defense in depth and defense in breadth.

Can explain the different uses of tactical risk treatment controls, for example, in a preventative, detective, corrective and / or directive implementation, and has a good knowledge of different types of operational risk treatment in terms of physical, technical and procedural / personnel and their appropriate uses.

Has knowledge of the application and implications of the most common regulations, standards, and legislation applicable in cyber security in the UK, for example: ISO/IEC27000 series, PCI/DSS, GDPR, DPA, Cyber Essentials.

Understands the need and principal concepts of threat intelligence and how it can aid an organisations overall information security.