

Standard of Professional Competence and Commitment:

Cyber Security Governance and Risk Management

Contents

Cyber Security Governance and Risk Management Contextualisation	1
▶ Acronym List.....	2
▶ Introduction	2
▶ Assessment.....	Error! Bookmark not defined.
▶ Contextualisation Table	Error! Bookmark not defined.

▶ ACRONYM LIST

Council	UK Cyber Security Council
ChCSP	Chartered Cyber Security Professional
PriCSP	Principal Cyber Security Professional
PraCSP	Practitioner 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 15 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), ISACA and ISC2 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**

Assessment will be against the competences described in the UKCSC SPCC using the below descriptions for context and following a registration process outlined in the UKCSC SPCC.

▶ **Contextualisation**

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

Practitioner	Principal	Chartered
<p>Can explain and give examples of the principles and practice of the risk management process as operated in employer, such as:</p> <ol style="list-style-type: none"> 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. 	<p>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.</p>	<p>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.</p>
<p>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 and risk methodologies, to determine those risks which are most applicable and consistent with the contextual requirements. Has completed risk assessments.</p>	<p>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.</p>	<p>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.</p>
<p>Can demonstrate the use of qualitative and/or quantitative risk analysis and the advantages/disadvantages of the technique used. Can define the terms risk appetite and</p>	<p>Recognises the limitations of risk analysis, for example for the determination of threat motivation, reputational impact, or complex system dynamics. Recognises the benefits of</p>	<p>Recognises the limitations of risk analysis, for example for the determination of threat motivation, reputational impact, or complex system dynamics. Recognises, and can explain</p>

Practitioner	Principal	Chartered
risk tolerance and how they are applied in the organisation in which they operate.	presenting alternative scenarios that elicit alternative risk dynamics.	in detail, the benefits of presenting alternative scenarios that elicit alternative risk dynamics.
Can explain in examples from their work, the risk treatment (treat, transfer, accept, etc.) applied and when each may be applicable. Can explain the terms likelihood and impact and how these have affected the risk rating in some of the work the candidate has completed.	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.
Can give suitable examples from their work of the different risk treatment controls, for example, 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 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 give practical examples of when regulation or standards (for example ISO/IEC27000 series, PCI DSS, GDPR, DPA, Cyber Essentials) has affected the work they have completed	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.

Practitioner	Principal	Chartered
	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.