UK CYBER SECURITY COUNCIL®

Standard of Professional Competence and Commitment:

Secure System Architecture & Design

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 describe meaningfully straight-forward security concepts and their business applicability together with a clear awareness of the need to provide traceability between business need and security requirements.	Clear awareness of the need to provide traceability between business need and security requirements.
The ability to contextualise security recommendations and risk statements to the business need under consideration.	The ability to review architectures and identify likely attacks with complex security requirements for non-standardised use cases. While this may use some well-established guidance, it is expected that at this level there will be novel elements outside existing guidance. (They could be contentious and need persuasive techniques to implement.)
The ability to review architectures and identify likely attacks for simple or obvious security requirements for highly standardised use cases, using well-established guidance.	The ability to provide advanced security architecture designs to address unusual or complex security needs. It is expected that the solutions are novel or high risk/impact and cannot just be implementations following standard patterns. Advice could be written or verbal.
The ability to provide security architecture designs to address standard security needs.	An awareness of limitations and scope for what advice can be given and when to draw on subject matter experts' expertise.

Principal	Chartered
The ability to support security professionals in designing secure systems and developing mitigation strategies for relatively common and well-understood scenarios.	The ability to support security professionals in designing secure systems and developing mitigation strategies for unusual and unique scenarios that are high risk or high complexity.
An awareness of the limitations and scope for what advice can be given and when to draw on others' expertise.	A complete and thorough understanding of risk, risk management processes and decision making. This can be met through: • The application of advanced security architectures in order to mitigate security risks; or • The ability to review system security architecture designs to ensure they mitigate identified complex or unusual security risks, whilst balancing an organisation's business requirements, e.g., reviewing complex or unusual systems to ensure that cyber-attacks are mitigated to a reasonable level, (set by the system owner) whilst balancing other factors such as user needs, costs, performance, etc.
An understanding of the fundamentals of risk, risk management processes and decision making; This can be met through: • The application of risk assessment and risk management techniques, coupled with good technical knowledge, to system designs in order to mitigate security risks; or • The ability to review security architecture designs to ensure they mitigate identified security risks, whilst balancing an organisation's business requirements, e.g. reviewing systems to ensure that cyber-attacks are mitigated to a reasonable level,(set by the system owner) whilst balancing other factors such as user needs, costs, performance, etc.	The candidate's architectural approach: • Understanding risk and how it drives designs; • Business owners, risk owners and wider stakeholder understanding and management; • Threat actors – how "secure" you need to make it; • Security benefit vs cost; • Identification and management of inputs (requirements, constraints, legal, principles, assumptions, etc.); • Design process – from inputs/requirements to design HLD/LLD, testing, TTO, BAU, maintenance, decommissioning; • Architectural principles – what they are, and the value they have; • Traceability between business need and security requirements; • Engaging and influencing non-security stakeholders and wider team members; • Having a vision and breaking it down into steps;

Principal	Chartered
	• Governance – managing change and expectations; • How to work in an agile world.
	The ability to describe meaningfully more complex security concepts and their business applicability.
	The ability to contextualise security recommendations and risk statements to the business need under consideration. This includes the ability to communicate complex technical matters in plain English when communicating with those outside the field of cyber security.