UK CYBER SECURITY COUNCIL®

Standard of Professional Competence and Commitment:

Security Testing

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, is 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. There 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 The Cyber Scheme and CREST, 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

The evidence for each professional title in this specialism will be provided either through the exiting examination process or via attestation. Any organisation providing attestation for a candidate must have signed up to a Code of Conduct, and/or Code of Ethics either directly with the Council, or with a Licensed Body.

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 an 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. Associate Cyber Security Professional is being developed. This document will be updated when Associate title is launched.

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
Good understanding of the lifecycle of different types and complexities of engagement.	An excellent understanding of the lifecycle of all types and complexities of engagement, including techniques for influencing a client through articulation of the benefits of cyber security testing.
Define and describe the scope and objectives of a security test for a large and/or complex environment.	Define and describe the scope and objectives of any security testing engagement, including large and complex tests involving multiple environments and technologies.
Have a good understanding of the common legal and regulatory frameworks relevant to security and IT environments and should have an excellent knowledge of the framework/s relevant to their specialism.	Have a thorough knowledge of the common legal and regulatory frameworks relevant to security and IT environments and should have an excellent knowledge of the framework/s relevant to their specialism/s.
Have a good understanding of business risk as it applies to security weaknesses and controls.	Have a thorough understanding of the risks involved in testing, and of the business risks related to findings and their mitigations.

Principal	Chartered
Demonstrate the ability to create appropriate test platforms for different types and complexities of test, including their own specialism and at least one other.	Demonstrate a thorough understanding of the setup of multiple test platforms, including within team-based testing, and the need for all hardware, cabling, software, licensing, sandboxes and sanitation.
Keep clear, concise, and accurate records of their test activities including descriptions of the repeatability of a finding, and how to classify findings.	Demonstrate a thorough understanding of the importance of clear, concise and accurate records of all aspects of a test and ensure that quality of record keeping is maintained by the test team.
Be able to determine whether a finding is sufficiently critical to warrant notification to the client immediately, at the end of day, or in the final report; and to demonstrate clear, concise, and accurate reporting in the final report.	Be able to determine whether a finding is sufficiently critical to warrant notification to the client immediately, at the end of the day, or in the final report; and to demonstrate clear, concise and accurate reporting in the final report; to be able to convey clearly to the client (who may be non-technical) what any finding means in terms of security posture and exposure to risk, and possible methods of mitigation.
Be able to present findings to senior management (i.e., CISO) comfortably.	Be able to present at Board level technical findings and assessment thematic comfortably.