UK CYBER SECURITY COUNCIL®

Standard of Professional Competence and Commitment:

Cyber Security Audit and Assurance

The Professional

Contents

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, 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 15 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 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

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.

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 document 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
Ability to explain through practical knowledge, the difference between assurance and audit (Possibly using the IIA's Three Lines Model - previously called Three Lines of Defense). Able to position their current experience (Audit or Assurance or both) and the value of each.	Ability to participate in and contribute to planning an organisation's cyber security audit activities.	Ability to contribute strategically to the organisation as a source of technical guidance and interpretations in respect of audit of cyber security risks management approaches and controls.
Can explain how an organisation can gain and maintain assurance/confidence in cyber security. These might include ways to gain and maintain assurance in people, processes, third parties and technology.	Ability to plan and manage audit engagements through the audit life cycle using an established audit framework, e.g., ISACA's IT Audit Framework (ITAF), ensuring adequate and proficient coverage and staff.	Ability to develop strategic plans to support assessment of regulations, standards, and legislation applicable to the business environment, in relation to cyber security audit.
Knowledge of security concepts associated with information technology assurance along with an understanding of risk management methods and security controls. Show through experience of explaining cyber security concepts to non-specialist colleagues or customers.	Ability to assess quality of fieldwork, audit evidence and conclusions of IT and cyber security audits.	Experience communicating audit progress, findings, results, recommendations and other audit matters to executives and the board with consideration given to perspectives of all stakeholders.
Show through practical application in your audit or assurance experience how applicable laws and regulations, policies and procedures (for example Computer Misuse act, PCI DSS or others that apply to your organisation) affect and influence the work completed. Show how	Ability to collaborate with groups across the organisation to ensure audit involvement in new initiatives and implementations and, when required, provide independent consulting services and guidance to the organisation on audit related topics.	Ability to develop and define strategies for investigations of fraud and other inappropriate organisational behavior.

Practitioner	Principal	Chartered
your practical experience covers people, process and technology controls. Explain through your practical knowledge how your organisation's method of completing audit and assurance is in accordance with generally accepted standards and a risk- based cyber security audit/assurance strategy.		
Ability to perform IT and cyber security audits/assurance (individually or as part of a team) in a timely manner, consistent with agreed scope, objectives, test and/or audit plans. Ability to explain findings to the audit/assurance lead/customer in a clear and concise way in such a way (in writing and verbal) and to articulate the purpose of root cause analysis as to enable a decision on the action (if any) to take.	Ability to contribute to the organisation as a source of technical guidance, interpretations, and trusted advisor, on matters relating to cyber security audit.	Ability to ensure that ethical standards are maintained by the team.
Ability to show through your work experience how your organisation's approach to audit /assurance uses or is influenced by (external) cyber security frameworks, for example NIST CSF, CAF, COBIT, ECSF), standards, for example ISO/IEC 27001, and industry good practices	Ability to apply critical thinking strategically and realise change through evaluation of IT strategy, resources, and portfolio management for alignment with organisational strategies and objectives, in relation to cyber security audit.	Ability to ensure that audit team maintain and develop necessary technical competence, skills and knowledge to support the cyber security audits.

Practitioner	Principal	Chartered
Explain through your practical knowledge and experience how supply chains influence the approach to managing cyber security audit / assurance, including, for example, enterprise IT systems, operational technology systems and cloud services.. This could also include ensuring that appropriate measures are employed where third party services are used.	Ability to evaluate the cyber security program to determine its effectiveness and alignment with the organisations strategies and objectives.	
Explain how your audit/assurance approach is influenced/affected by organisational business resilience requirements (depending on the risk profile in your organisation and the regulatory requirements covering your organisation this may include, for example, DORA, PRA regs, NIS regs and immutable backups).	Ability to perform (or assist in performing) special projects, such as fraud investigations.	
Ability to demonstrate good communication skills both verbally and in writing.	Ability to communicate technical information (and/or large amounts of business information) into succinct, business centric language.	
Ability to conduct interviews showing sufficient empathy and understanding to feed back during the review. Ability to take sufficient notes (or recordings then notes) to ensure that topics need not be covered more than once.	Broad knowledge of IT industry trends, emerging technologies, and cyber security threat landscape to assess actual and potential threats and associated techniques in the organisation's IT and business processes.	

Practitioner	Principal	Chartered
Demonstrate understanding and importance of evidence based review and sampling techniques.	Ability to solve problems and manage multiple projects simultaneously.	
	Ability to demonstrate exceptional communication skills. For example, it is important to be able to explain any residual risks that the audit has uncovered and the ability to relate that to the impact on the business.	