Standard of Professional Competence and Commitment:

Cyber Security Audit and Assurance

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 Chartered Institute of Information Security (CIISec) 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

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.

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
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.
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.
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.
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.

Principal	Chartered
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 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.
Ability to evaluate the cyber security program to determine its effectiveness and alignment with the organisations strategies and objectives.	
Ability to perform (or assist in performing) special projects, such as fraud investigations.	
Ability to communicate technical information (and/or large amounts of business information) into succinct, business centric language.	
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.	
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.	

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

Associate
Ability to explain the IIA's Three Lines Model (previously called Three Lines of Defense) and Internal Audit's role in the third line as an Assurance function, that is as an independent function reporting directly to the highest point of authority in the organisation – the governing body (audit committee) – providing advice, insight, and continuous improvement, and at the same time supporting management in their role.
Ability to describe the different ways in which an organisation might be able to gain and maintain assurance/confidence in their approach to cyber security. These might include ways to gain and maintain assurance in people, processes and technology.
Knowledge of security concepts of information technology assurance, the risk management processes and security related controls.
Ability to review information technology systems and associated processes and controls for alignment with strategic objectives and compliance with applicable laws and regulations, for example GDPR, PCI/DSS and DPA, and policies and procedures.
Ability to conduct audits in accordance with generally accepted audit standards and a risk-based cyber security audit strategy.
Ability to perform IT and cyber security audits (individually or as part of a team) in a timely manner, consistent with audit scope, objectives and testing plans.
Ability to perform audit tests to confirm that cyber security related controls are operating effectively and to identify missing controls.
Ability to evaluate IT and business management's monitoring of controls.
Ability to evaluate management's monitoring and reporting of key cyber security related metrics.
Knowledge of (internal) information security, cyber security and privacy policies.
Knowledge of relevant (external) cyber security frameworks, for example NIST CSF, CAF, COBIT, ECSF), standards, for example ISO/IEC 27001, and industry good practices.
Awareness of the technical and non-technical controls that are used to manage cyber security risks to technology systems and their supply chains including enterprise IT systems,

Associate
operational technology systems and cloud services. This includes ensuring that appropriate measures are employed where third party services are used.
Awareness of business resilience concepts including business continuity planning and disaster recovery.
Ability to perform duties with objectivity, due diligence and professional care, in accordance with professional standards and guidelines, e.g., ISACA's Information Systems Auditing Standards and Information Systems Auditing Guidelines.
Ability to demonstrate good communication skills.
Ability to conduct interviews.