UK CYBER SECURITY COUNCIL®

# Standard of Professional Competence and Commitment:

# Secure Operations

T

# 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, 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 various 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 SANS 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.

Secure Operations ensures end-to-end management of an organisation's networks and systems, ensuring they operate and meet the required security policies, standards, and any applicable regulations. Activities will include systems that may also be running in cloud environments. Agreed-upon policies, standards, controls, processes, and procedures underpin all monitoring activities of secure operations and ensure confidentiality, integrity, and availability across all information systems. User access, authentication, and authorisation, and supporting specific areas of the incident management process also relate to activities for secure operations.

Secure Operations delivers and operates its management processes guided by the organisation's agreed policies, standards, and controls. Collaboration is at the heart of all operations, ensuring relativity and alignment when setting standards and controls across all functional and operational lines. The importance of agreed roles and responsibilities with users across the organisation means secure operations are better able to have a good understanding of areas such as system and business ownership, as well as the importance of all information created, processed, transported and or stored on all systems.

This specialism encompasses:

This specialism covers all aspects of network and system configuration, security tooling and systems, risk, and incident management, including operating in VM environments and knowledge of Identification and Access Management (IDAM). It also includes knowledge of the importance of Security Incident Event Management (SIEM) operations, understanding the role and operations of Security Operations Centres (SOC).

The cyber security specialist at both the Principal and Chartered levels must work across all areas of an organisation (e.g., risk and incident management, architecture, design, and operations), interact with and collaborate with users to find solutions for compliance with security policies and meet standards and controls.

## Assessment

In line with other specialisms, of the competences described via the UKCSC SPCC, the candidate will be expected to demonstrate thorough understanding of competence areas based on the candidate's body of work; a combination of experience, capabilities, education, and certification.

## 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. The Principal

guidance below builds on the Practitioner category, expanding the level and depth of competence expected to be demonstrated.

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 Assessors throughout the process will be using this guide as the basis for their questioning and challenging to assess the level of knowledge, understanding and personal experience in each area.

| Practitioner | Principal | Chartered |
|---|---|---|
| Can demonstrate evidence of experience working on various cyber security systems / technologies. This includes actively participating in monitoring, configuring and maintenance of those systems to protect organisational assets from cyber threats. [A1] | Is able to describe the key security configuration elements associated with the configuration and maintenance of networks and systems [A1] | Can describe the critical security configuration elements associated with the configuration and maintenance of networks and systems [A1] |
| Demonstrate experience of following process/procedures to;<br><br>Maintain systems to ensure they deliver expected services, and;<br><br>Handle some areas of risk management. [A2] | Ability to outline the key areas and processes for risk management. [A2] | Ability to outline understanding and contribute to risk management. [A2]. |
| Ability to identify configuration items in system management and their role in maintaining the overall system integrity. [A3]<br><br>Possesses sufficient understanding to support basic security operational tasks, such as assisting in detection and response practices/efforts during an investigation or incident. [A3] | Ability to provide a walkthrough of security operational investigation, including detection and response processes. Includes the use of threat intelligence information in all stages of an incident response [A3] | Ability to provide a walk-through of security operational investigation, including detection and response processes. Includes the use of threat intelligence information in all stages of an incident response. [A3]<br><br>Experience in designing and refining detection and response processes in support of investigations and incidents [A3] |
| Demonstrate understanding of the fundamental principles of Identity and Access Management (IDAM) and associated architectural solutions. Identify key processes and technologies that support methods such as authentication, authorisation, and | Is able to outline the technology, processes and procedures associated with areas such as Identity and Access Management (IDAM) and architectural solutions that support methods such as authentication, authorisation, and accountability for all systems. Knowledge should include how remote | Outline the technology, processes and procedures associated with areas such as Identity and Access Management (IDAM) and architectural solutions that support methods such as authentication, authorisation, and accountability for all systems. Knowledge should |

| Practitioner | Principal | Chartered |
| --- | --- | --- |
| accountability, including their application in remote and distributed systems. [A4] | and distributed systems across the operational and functional lines. [A4] | include how remote and distributed systems integrate with these solutions.<br><br>Can describe how solution and strategic implementation plans develop (working across the operational and functional lines.) [A4] |
| Understand the security requirements to maintain a secure virtualisation environment [A5] | Identify the security requirements to create and maintain a secure virtualisation environment. [A5] | Demonstrate expertise in designing, implementing, and overseeing comprehensive security strategies for virtualization environments. [A5] |
| Demonstrate an understanding of foundational networking protocols and cryptographic protocols, including their role in securing communications and data. [A6] | Outline the functionality and application of key networking protocols and demonstrate a comprehensive understanding of cryptographic protocols. [A6] | Demonstrate expertise with networking and cryptographic protocols. Lead the implementation of secure networking solutions to address complex security challenges. [A6] |
| Understand the key areas and elements that make up a distributed system environment e.g. event systems, peer-to-peer systems, and cloud knowledge, which includes the principles of operating in a multi-cloud operating environment [A7] | Ability to describe the key areas and elements that make up a distributed system environment, e.g. event systems, peer-to-peer systems, and cloud knowledge, which includes the principles of operating in a multi-cloud operating environment. [A7] | Ability to describe the key areas and elements that make up a distributed system environment, e.g. event systems, peer-to-peer systems, and cloud knowledge, which includes the principles of operating in a multi-cloud operating environment. [A7] |
| Demonstrate understanding of principles and processes that are part of the forensics process such as data collection, the chain of custody and the processes that may support any data analysis requirements. [A8] | Is able to outline the main principles and conduct the processes that are part of the forensics process such as data collection, the chain of custody and the processes that may support any data analysis requirements and initial investigations as required. | Can describe the main principles and lead the processes that are part of the forensics process such as data collection, the chain of custody and the processes that may support any data analysis requirements and investigation. [A8] |

| Practitioner | Principal | Chartered |
|---|---|---|
| | [A8] | |
| | Is able to describe and show and understanding of malware and attack environments such as distributed malicious systems and associated discovery and analysis procedures [A9] | Is able to describe and show an understanding of malware and attack environments such as distributed malicious systems and associated discovery and analysis procedures [A9] |
| | Is able to understand key firewall configuration requirements and processes relating to Security Incident Event Manaegment (SIEM). This knowledge should include patch and backup management policies. [A10] | Demonstrate thorough understanding of SIEM platforms.<br><br>Demonstrate expertise in various aspects, this includes proficiency in configuring and managing SIEM tools, ability to integrate data sources for comprehensive log aggregation, knowledge of event correlation to identify and prioritise security incidents. [A10] |
| | Ability to outline the key principles of technical vulnerability assessments. [A11] | Ability to understand the key principles of technical vulnerability.<br>assessments. [A11] |
| | Can describe the operating principles of a Security Operations Centre (SOC). [A12] | A thorough understanding of the operating principles of a Security Operations Centre (SOC). [A12] |
| | Can describe key areas for collaboration with the physical security environment for areas which may relate to the administration of logical and physical user access rights [A13] | Can itemise some key areas for collaboration with the physical security environment for areas which may relate to the administration of logical and physical user access rights [A13] |
| | Outline the key areas for conducting vulnerability | Describe the key areas for conducting |

| Practitioner | Principal | Chartered |
|---|---|---|
| | assessments and any outcomes of data protection analytics and required remediation solutions. [A14] | vulnerability assessments and any outcomes of data analytics and required remediation solutions. [A14] |
| Demonstrate experience of system management by effectively implementing the deployment, configuration and maintenance of the systems and networks throughout the system lifecycle. [A15] | Demonstrate good understanding of system management by effectively overseeing the deployment, configuration and maintenance of the systems and networks throughout the system lifecycle. [A15] | Demonstrate thorough understanding of system management by effectively overseeing the deployment, configuration and maintenance of the systems and networks throughout the system lifecycle. [A15] |
| Demonstrate understanding and be familiar with organisational approved frameworks. [A16] | Demonstrate good understanding of cyber security frameworks and ability to identify suitable frameworks in different organisational and regulatory contexts. [A16] | Demonstrate thorough understanding of cyber security frameworks and ability to identify suitable frameworks in different organisational and regulatory contexts. [A16] |
| | Demonstrate understanding of the MITRE ATT&CK framework.<br><br>Explain how the framework can be used to integrated into threat intel and threat emulation. [A17] | Demonstrate a comprehensive understanding of the MITRE ATT&CK framework.<br><br>Explain how the framework can be integrated into threat intel and threat emulation. [A17] |
| | Demonstrate good understanding of cyber security frameworks and ability to identify suitable frameworks in different organisational and regulatory contexts. [A18] | Demonstrate thorough understanding of cyber security frameworks and ability to identify suitable frameworks in different organisational and regulatory contexts. [A18] |
| Demonstrate ability to follow the change process. [A19] | Demonstrate ability to assist with the design, implementation, and management of secure operations processes / procedures, ensuring systems and networks deliver expected services. | Demonstrate ability to lead the design and manage secure operating process/procedures, ensuring that systems and networks deliver expected services. |

| Practitioner | Principal | Chartered |
|---|---|---|
| | Ability to assist with the created plans for implementation management. [A19] | Ability to evaluate and sign off the configuration management plan (i.e. Configuration Items) to track and maintain system configurations. [A19] |
| Demonstrate experience of system management by effectively implementing the deployment, configuration and maintenance of the systems and networks throughout the system lifecycle. [A20] | Demonstrate good understanding of system management by effectively overseeing the deployment, configuration and maintenance of the systems and networks throughout the system lifecycle. [A20] | Demonstrate thorough understanding of system management by effectively overseeing and having responsibility for the deployment, configuration and maintenance of the systems and networks throughout the system lifecycle. [A20] |
| Demonstrate evidence of using SIEM / XDR or related technologies (such as Honeypot types), to detect and respond to anomalies and security events.<br><br>Ability to analyse security logs and alerts to identify potential threats and operational issues.<br>[A21] | Demonstrate comprehensive understanding of using SIEM / XDR or related technologies (such as Honeypot types) to detect and respond to anomalies and security events.<br><br>Ability to analyse security logs and alerts to identify potential threats and operational issues. [A21] | Demonstrate a thorough understanding of a SOC.<br><br>Demonstrate ability to understand complex security architecture by analysing and integrating various components such as network infrastructure, security controls, and data flow.<br><br>Able to address issues within the integration process. [A21] |
| Demonstrate an understanding how data science techniques and user/entity behaviour analytics can have an impact on how risks are identified in the SIEM data. [A22] | Demonstrate comprehensive understanding how data science techniques and user/entity behaviour analytics can have an impact on how risks are identified in the SIEM data. [A22] | Demonstrate thorough understanding how data science techniques and user/entity behaviour analytics can have an impact on how risks are identified in the SIEM data. [A22] |
| Ability to follow a process to gather and deliver threat intelligence. [B1] | Ability to develop a process to evaluate and contextualise threat intelligence to deliver the threat intelligence. [B1] | Ability to communicate insights derived from threat intelligence to technical and non-technical stakeholders. [B1] |

| Practitioner | Principal | Chartered |
|---|---|---|
| | | |
| | demonstrate skills in conducting compliance assessments and ensuring organisational adherence to relevant regulations i.e. Secure by Design principles [B2] | demonstrate good understanding of project management process, particularly in the context of technical projects, ability to oversee the project lifecycle and ensure that the requirements are met while adhering to standards. [B2] |
| | Demonstrate ability to collaborate effectively with stakeholders, both technical and non-technical to ensure a comprehensive approach to security. [B3] | Can lead, manage, and develop people through coaching and mentoring. Can create and lead formal or informal teams and /or create collaborative links with teams. Provides support and feedback to encourage and develop colleagues.<br><br>Advises and influences others. [B3] |
| Demonstrate understanding of how solution plans for implementation can develop across operational and functional lines. [C1] | Can describe how solution and strategic plans for implementation develop (working across the operational and functional lines). [C1] | Can manage resources, people, and budgets in complex and high-pressure cybersecurity environments. [C1] |
| Demonstrate relevant communication to direct management, security professionals and internal + external stakeholders, etc. [C2] | Demonstrate communication at all levels including, but not limited to, C-Suite level, senior management, security professionals etc, in a deputised capacity. [C2] | Demonstrate communication at all levels including, but not limited to, C-Suite level, senior management, security professionals etc. [C2] |