UK CYBER SECURITY COUNCIL®

Standard of Professional Competence and Commitment:

Secure Systems Development

DEFINITIONS

Council	UK Cyber Security Council
ChCSP	Chartered Cyber Security Professional
PriCSP	Principal Cyber Security Professional
PrsCSP	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 Council is a Royal Chartered organisation that 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 initiative, it is important that the Council creates a vibrant and diverse cyber security profession, 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 contextualisations across 16 industry areas to support professional registration. These 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 The Institute of Engineering and Technology (IET), and BCS, The Chartered Institute for IT. The document aims to contextualise the overarching standard, showing the typical types of working evidence required to meet the competence and commitment statements for the professional titles listed in the UKCSC SPCC.

Assessment

In line with other specialisms, the candidate is expected to demonstrate a thorough and detailed knowledge of at least 80% of the competences described via the UKCSC SPCC. For the remaining 20%, the candidate must demonstrate, at minimum, a lower but acceptable level of understanding.

Introduction

Secure Systems Development is the technical work that delivers and maintains software and/or hardware, in conformance with agreed security requirements and standards, throughout its lifecycle. It is closely related to the Secure Systems Architecture and Design and Testing Specialisms.

Secure Systems Development is a fundamental part of creating new products, systems and services that form the bedrock of our economy – from telecommunications, through utilities to transport infrastructure. Increasingly these sectors are being targeted by a range of hostile actors including criminals, hacktivists, and nation states. The impact of an attack can be wide ranging: from disruption, loss of data, economic damage through to loss of life.

Secure System Development involves thinking about cyber security from the outset with the aim of reducing the impact of potential cyber-attacks, reducing user error, increasing resilience, and reducing whole-life costs. This approach is scalable and spans low-cost consumer Internet of Things (IoT) products through to large-scale complex control systems for a nuclear power station.

This specialism encompasses **[A1 to A10]:**

1. Developing a solution to meet user needs: capturing requirements, assessing human factors, managing risk, threats, safety, and legal compliance.
2. Managing supply chain risk (up and downstream).
3. Securing the build environment.
4. Reviewing designs, code inspection and testing.
5. Managing change effectively.
6. Building for through-life, as the threat landscape will change.
7. Employing a sustainable approach to development.
8. Hardening a system to counter digital threats.

The Council has also listed expectations on Communication [D1]. This specialism builds security into engineering design, development and production processes, giving stakeholders the assurance that appropriate steps have been taken to manage risk in line with the threat and impact. The Council's approach is standards agnostic.

Underpinning Knowledge and understanding

The Council is currently developing the Cyber Security Qualification Framework to improve the navigability of the cyber security learning and application landscape. Whilst this work is ongoing, there is a need to provide reference in outline to the expected level of knowledge, skill, experience, attitudes, and behaviours against the 3 professional registration titles that could be met through qualification, expertise, experience, or a mix of all. Updated information can be found on the Council's website here:

https://www.ukcybersecuritycouncil.org.uk/professional-standards-registration/standard-for-professional-competence-and-commitment/

Contextualisation

The table below provides a comparison of the types of evidence and level of competence an individual must demonstrate for the two professional titles: Chartered Cyber Security Professional and Principal Cyber Security Professional.

The guidance below builds upon the level described for the Principal category, and expands the depth of competence that needs to be demonstrated by someone meeting the Chartered category of professional registration.

This should not be viewed as a checklist, but as a guide to the areas of knowledge and experience that need to be demonstrated. The interviewers will be using this guide as the basis for assessing the candidate's level of knowledge and understanding in each competence area.

Practitioner	Principal	Chartered
	A1 The ability to describe and demonstrate how system designs are progressed from inception through to whole life service based on systematic ‘develop-test-build-operate’ methodologies. Expected to demonstrate how end user requirements are captured, how security attack vectors are considered (both qualitative and quantitative assessments) throughout system life cycle. Expected to demonstrate what risk methodologies are deployed e.g. Carver etc, how threats, vulnerabilities and mitigation aspects are managed (across system life cycle) and thus embedded within a system design from the outset. At the planning stage, is able to provide evidence of knowledge and the understanding of the importance of incorporating the areas of security, risk, threat, and vulnerability management as part of the requirements capture process. Expected to demonstrate the impact of system security considerations on legislated safety requirements, and legal compliance. Describe approach to solving problems and use of research and innovation. Ability to contextualise how third-party security factors i.e. outside of the direct scope of a secure	**A1** Consideration of various ‘*develop-test-build-operate*’ methodologies and their respective merits to a security system design use case. Being able to describe the respective ‘*qualitative and quantitative*’ assessment methods and their respective merits. Application of risk methodologies to manage high risk/complexity along with their respective merits to a security system design use case. Demonstrate where they have used research and innovative techniques in developing a secure system. Demonstrate and describe a number of contextualised approaches on how a secure system needs to perform during its life cycle within the built environment. As part of the planning phase and requirements capture process, there must be the knowledge to lead discussions on the

Practitioner	Principal	Chartered
	system, are both considered and then embedded within the system design. Examples could include how use-case and work-flow analysis tools are utilised to forecast the cyber security performance within the wider built environment.	elements of the security risk management process and the controls that security will implement to form part of the end-to-end system development process. Must also be able to explain how the output from control testing will support seamless security integration throughout the development lifecycle process.
	A2 Describe whole life methodologies of managing supply chain risk. Being able to describe how system designs ensure that risks attributed to procurement, build, test and distribution within a supply chain are considered and managed, and what tests are deployed to ensure probity and authentication of the outturn secure system.	**A2** Consideration of various supply chain models and their respective security merits in relation to a security system design use case. Understanding the provenance of 3rd party hardware and code. Demonstrate and consideration of the most appropriate supply chain security control mechanisms that need to be in place throughout secure system lifecycle (and their respective merits).
	A3 Demonstrate understanding of the people, process, physical and technical controls required for secure development. This includes human factors (in a security context), cyber controls for networks; secure information management (including access by 3rd parties); and screening of staff. Demonstrate a layered approach to security which includes developing with the end-user in mind, ease of	

Practitioner	Principal	Chartered
	use, considering compartmentalisation, human factors, use of reference systems, digital twins and digital design information.	
	A4 Demonstrate and discuss how system designs and development methodologies are reviewed against all cyber security and other impacting criteria i.e. commercial, legal, compliance etc (as set out in A1) and considerations of how the embodiment of a proven quality control & change management system has been utilised to ensure efficacy of the secure system is maintained.	**A4** Demonstrate understanding of how corporate goals are married alongside a secure system design. Examples would include reputation management, risk ownership and risk transfer considerations.
	A5 & 6 Demonstrate and describe how unknown downstream threats and mitigations are communicated and potentially resolved during system lifecycle (from inception to decommissioning). Consideration of what design slack and security tolerances exist within a system which could potentially be deployed as part of a forward-thinking mitigation capability. Is able to demonstrate knowledge and experience for maintenance steps that should be in place to support adaptability throughout the lifetime of the system.	**A5 & 6** An appreciation that can be demonstrated and described of how unknown downstream threats and mitigations are communicated and potentially resolved during system lifecycle. Consideration of what design slack and security tolerances exist within a system which could potentially be deployed as part of a forward-thinking mitigation capability.

Practitioner	Principal	Chartered
	A7 Understand the principles of sustainable development and apply them in their work. This is a wide-ranging topic and could include energy efficiency, waste reduction and sustainable sourcing. Understand and demonstrate knowledge of the process and procedures to ensure any system's secure and safe retirement. This knowledge should include the elements for both the system and the data components.	**A7** Hardening a system to counter digital threats. Describe how defensive design enhances a system's ability to recognise abnormalities and respond safely. Explain how systems are built and configured for correctness and high availability. Can provide the thought process that underpins integrating the applicable cyber security knowledge into all areas of a chosen system design.
	A8 Describe the threats that apply to a system as it executes and demonstrate an understanding of the technical controls displayed to counter these threats. Discuss how complementary countermeasures provide defence in depth.	**A8** Describe how defensive design enhances a system's ability to recognise abnormalities and respond safely. Explain how systems are built and configured for correctness and high availability.
	A9 The ability to support security professionals in designing secure systems and developing mitigation strategies for relatively common and well-understood scenarios.	**A9** The ability to lead security professionals in designing secure systems and developing mitigation strategies for relatively common and well-understood scenarios. Can provide the thought process that underpins integrating the applicable cyber security knowledge into all areas of a chosen

Practitioner	Principal	Chartered
		system design. e.g. Intrusion Detection Systems(IDS), encryption levels if relevant.
	A10 Fully cognisant of commercial and system performance requirements and being able to demonstrate how system design considers these factors and then balances the outturn security posture against commercial and performance constraints.	**A10** Demonstrating the lead decisions on commercial and system performance requirements and leading on the balance between security posture against commercial and performance constraints.
	D1 Describe the limitations and scope for what advice can be given and when to draw on others' expertise.	**D1** Being able to demonstrate how current limitations of security capability and posture (given commercial and corporate constraints) are challenged and improved upon. Benefits vs risk.