

Standard of Professional Competence and
Commitment:

INCIDENT RESPONSE

T

Contents

Incident Response Contextualisation.....	1
Acronym List.....	2
Introduction	2
Assessment.....	3
Contextualisation Table.....	3

| 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, 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. 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 The Cyber Scheme, CREST, SANS and IASME, 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 a 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.

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.

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.

Competence Reference from UKCSC SPCC	Principal Example of evidence	Chartered Example of evidence
Competence A: Knowledge, Understanding & Experience	<ul style="list-style-type: none">• Possess a broad technical understanding of the relevant subject matter and what the different areas involve.• Has ability to draw on knowledge and personal professional experience to input into the incident action plan, associated incident playbooks and can execute them with minimum direction.• Understands the core technical concepts related to the discipline and apply them appropriately with minimal guidance.	<ul style="list-style-type: none">• Has a deep subject matter knowledge across key incident response specialist areas and can demonstrate understanding of the technical and procedural concepts, and their application.• Has real-world experience of incident management, either as an incident response team leader or an area specialist with a strong track record of managing incidents ranging from simple to complex, with responsibility for the full incident lifecycle, up to and including final sign off and liaison with the entity under investigation.• Although they may not be specialist across every specialist area, they can understand the

Competence Reference from UKCSC SPCC	Principal Example of evidence	Chartered Example of evidence
		complementary parallel disciplines (to incident response), liaise with those team specialists and delegate taskings to them and review outputs from those teams with a high degree of competency and confidence.
Competence A: Knowledge, Understanding & Experience	<ul style="list-style-type: none"> • Understands the elements of a cyber incident and can apply the principles of incident management to undertake relevant courses of action to deliver the desired outcome. • Can provide guidance to an organisation on different solutions to a problem, whilst being independent and objective for the considerations for the situation. • Has the subject matter knowledge to resolve challenges faced before them and adequate experience to seek advice from colleagues or a team manager when required. 	<ul style="list-style-type: none"> • They can apply their knowledge and experience to new/unknown incident response situations and can apply their knowledge and the methodologies to tackle those situations with no difficulty. • Can take input from the customer and team members and apply their own knowledge and experience to formulate the plan and direction of an incident investigation. • Can both direct and execute the incident investigation, deal with unforeseen challenges, problems and customer inputs/constraints, whilst operating within the constraints of customer and regulatory/legal requirement.
Competence A: Knowledge, Understanding & Experience	<ul style="list-style-type: none"> • Understands the direction and required outcomes of the situation and can input into and execute tasks to enable the overall objectives to improving cyber security. • Can input into the creation of a cyber security improvement plan and can assist the organisation to achieve it. Has the experience and skills to feed into, update and create an incident action plan and associated incident playbooks. 	<ul style="list-style-type: none"> • Has real-world experience of implementation of remediation actions and improvements both to the incident management processes and more widely to cyber security. • Can manage customer and team expectations and stakeholder input whilst preparing and executing improvement plans for cyber security and work within the real-world situational constraints and limitations to get the best course of action

Competence Reference from UKCSC SPCC	Principal Example of evidence	Chartered Example of evidence
		<p>for improving cyber security under the circumstances.</p> <ul style="list-style-type: none"> • Can provide remedial and strategic advice to fill any located gaps in process, procedures and technology.
Competence B: Communications & Interpersonal Skills	<ul style="list-style-type: none"> • Presents feedback, plans, updates and recommendations to the organisation in a non-technical manner, using language appropriate to the audience. • Can explain and convey the main objectives and impact of a situation and what it means to the organisation without the need for technical jargon. 	<ul style="list-style-type: none"> • Can communicate with all different stakeholders to convey the relevant points about incident response and cyber security, whilst being sensitive to stakeholders' knowledge levels, role within organisation and experience. • Is comfortable and willing to challenge assumptions and inaccuracies where necessary, to do the right thing for the organisation and can receive and accept input from team members, peers and seniors, and apply it appropriately and objectively without prejudice.
Competence B: Communications & Interpersonal Skills	<ul style="list-style-type: none"> • Can extract the key elements of a finding or situation, provide considered feedback and justify it. • Can objectively explain to a non-technical audience the reason and impact of following and not following any advice given within the context of the organisation's situation. 	<ul style="list-style-type: none"> • Can act as a subject matter expert in incident response, with confidence and distinction to convey its complexities in a clear, concise manner to audiences of different backgrounds and abilities. • Can provide informed context, advice and guidance or otherwise reference other sources of information where required across all areas of incident response.
Competence B: Communications & Interpersonal Skills	<ul style="list-style-type: none"> • Has the ability and resolve to deal with all different types of people, with differing knowledge and stress levels during a cyber incident and has the ability to escalate to senior members of the team where necessary. 	<ul style="list-style-type: none"> • Has the ability to prevent and resolve conflicting situations, obtain the best results from team members and stakeholders across a multiple of situations relating to incident response.

Competence Reference from UKCSC SPCC	Principal Example of evidence	Chartered Example of evidence
	<ul style="list-style-type: none"> • Can demonstrate patience to and understanding of the stakeholder's situation and feelings whilst involved in a cyber incident. 	<ul style="list-style-type: none"> • Can act as the final escalation point for resolutions and direction of differing situations or opinions. • Can lead the team and stakeholders through a multitude of different situations and personal feelings during an incident to obtain the best and most productive results for all involved.
Competence B: Communications & Interpersonal Skills	<ul style="list-style-type: none"> • Can demonstrate that they can convey technical matters in a report format that is understood by a reader without the technical background. • Can explain verbally technical and complex matters in a way that helps the listener to understand the key take away points, without making them feel confused or technically inferior, or asking more questions as a result. 	<ul style="list-style-type: none"> • Can communicate clearly in written or verbal form to audiences ranging from senior executive to technical specialists and those with less business and technical experience. • Can quality-assure team outputs and deliverables to a high standard both for technical content and English language competency. • Can speak with and explain clearly all matters of incident response to any audience irrespective of their knowledge levels, role within organisation, experiences and stature, in a way that builds trust and confidence in the person and does not result in a negative or confused output.
Competence B: Communications & Interpersonal Skills	<ul style="list-style-type: none"> • Understands how to prioritise, set tasks, utilise planning methodologies and consider business requirements. Including costs, ROI and also how to justify the security investment within the context of the organisation. 	<ul style="list-style-type: none"> • Can assist in the final sign off and presentation of a plan, methodology or budget etc, whilst considering the wider organisational needs and constraints and with the ability to justify their decisions constructively and confidently. • Can work with any necessary changes seamlessly and is not afraid to push back and defend

Competence Reference from UKCSC SPCC	Principal Example of evidence	Chartered Example of evidence
		<p>or adapt their plan when required to do so.</p> <ul style="list-style-type: none"> • Can take input from team members and organisational contacts during these situations and utilise them for the benefit of the situation.
Competence C: Collaborative Management, Leadership & Mentoring	<ul style="list-style-type: none"> • Capable of delegating tasks, mentoring and guiding junior staff and sharing experience. • Is calm and considered in stressful and pressured situations and can support colleagues to get the best out of them. 	<ul style="list-style-type: none"> • Has real-world experience of leading teams, developing their skills and abilities and providing direction when required. • Can manage different personalities across numerous situations, often under pressure in stressful scenarios, with confidence and equality; taking into consideration the team's skill sets, backgrounds and abilities. • Can provide sources of reference to resolve problems and help mentor team members and has suitable knowledge to answer questions directly.
Competence C: Collaborative Management, Leadership & Mentoring	<ul style="list-style-type: none"> • Experience of formulating plans, setting tasks with deadlines both for team members and oneself. Capable of managing expectations including dealing with changeable situations. 	<ul style="list-style-type: none"> • Can provide direction, sign off and constructive criticism to ensure objectives, deadlines and organisational requirements are achieved on time and up to the necessary quality standard. • Can formulate and present plans to stakeholders and can manage problems, changes and limitations on the situation with ease resulting in a positive outcome.
Competence D: Integrity	<ul style="list-style-type: none"> • Ensuring professionalism at all times by not letting personal opinions influence any professional situations and 	<ul style="list-style-type: none"> • Promote good professional practice across team members, ensuring unbiased work is carried out at all times.

Competence Reference from UKCSC SPCC	Principal Example of evidence	Chartered Example of evidence
	<p>ensuring the needs of the entity under investigation is the number one priority.</p> <ul style="list-style-type: none"> • Ensuring that all data related to the case is kept secure and not shared with any other unauthorised party. • Making sure that the integrity of the entity under investigation and the case information is kept confidential at all times. 	<ul style="list-style-type: none"> • Ensure that all information is kept confidential both verbally and in written format. • Take responsibility for ensuring the security of the data related to the case is maintained and take ultimate responsibility for the integrity of the case and related information is kept confidential and not shared or discussed with unauthorised parties.
Competence D: Integrity	<ul style="list-style-type: none"> • Ensure the right action is undertaken at all times, ensure any mistakes are shared constructively and problems owned up to. No potentially negative situation is hidden or ignored to cover for mistakes. • Perform actions with the upmost integrity and independence and not be swayed or bribed in any way. 	<ul style="list-style-type: none"> • Ensure the values and standards are maintained within the team at all times and promote best practices and lead by example. • Provide guidance and resolutions to team members and organisational contacts where required on matters relating to integrity and honesty, and other points of professionalism or contention of a similar nature.
Competence D: Integrity	<ul style="list-style-type: none"> • Support diverse and inclusive recruitment practices, ensuring the avoidance of unconscious bias and advocating wherever appropriate for increasing the diversity of the cyber security profession. 	<ul style="list-style-type: none"> • Lead by example in the development of the Cyber Incident Response profession, advocating publicly for increasing the number of and diversity within the professionals in the cyber security community. • Challenges where necessary inappropriate behaviour within the profession, whether within their own organisation or other members of the cyber security community.
Competence E: Personal Commitment	<ul style="list-style-type: none"> • Read, understand, commit and comply with any relevant codes of conduct. Be able to understand where these fit 	<ul style="list-style-type: none"> • Ensure all team members read, understand, commit and comply with any relevant codes of conduct.

Competence Reference from UKCSC SPCC	Principal Example of evidence	Chartered Example of evidence
	<p>into their role and help junior team members to do the same.</p>	<ul style="list-style-type: none"> • Help the team and relevant stakeholders understand where these fit into their role and the relevant situations as appropriate. • Lead by example and promote the values and standards of the relevant membership organisations.
Competence E: Personal Commitment	<ul style="list-style-type: none"> • Read, understand, commit and comply with any relevant legal and regulatory requirements. Be able to understand where these fit into their role and help junior team members to do the same. 	<ul style="list-style-type: none"> • Ensure all team members read, understand, commit and comply with any relevant legal and regulatory requirements. • Help the team and relevant stakeholders understand where these fit into their role and the relevant situations as appropriate. • Lead by example and promote the relevant laws and regulatory requirements.
Competence E: Personal Commitment	<ul style="list-style-type: none"> • Understands the application of the standards and how they are used as part of their role and how they can be utilised for the entity under investigation. 	<ul style="list-style-type: none"> • Maintain up to date knowledge on trends and new developments within the industry to recognise new/upcoming standards that may be relevant as well as determining those that need application within the context of the organisation or team.
Competence E: Personal Commitment	<ul style="list-style-type: none"> • Ensure honest record keeping and audit trails of attendance of professional development. 	<ul style="list-style-type: none"> • Take responsibility for one's own professional development and those of their team members. • Ensure accurate record keeping occurs and quality assure the records and results of the professional development to ensure effectiveness and standards are maintained.

Competence Reference from UKCSC SPCC	Principal Example of evidence	Chartered Example of evidence
Competence E: Personal Commitment	<ul style="list-style-type: none"> • Attend public conferences, partake in discussions, assist in knowledge sharing and generally promote the profession. 	<ul style="list-style-type: none"> • Take the lead and promote the cyber security profession. • Provide through leadership, input and speak at public conferences sharing experiences and educate those around them. • Enable team members to partake and do the same.
Competence E: Personal Commitment	<ul style="list-style-type: none"> • Conduct continuous learning and research within the discipline and evolving threats and tactics. • Has the ability to keep up-to-date with threat intelligence and analysis. 	<ul style="list-style-type: none"> • Lead and promote continuous development within the future of cyber security and the associated trends, threats and technology evolutions. • Contextualises this knowledge and feeds this into the strategic guidance provided to the incident response team and entities within their area of operation. • Enable team members to do the same.