National Cyber Security Centre
a part of GCHQ

NCSC Certified Cyber Professional (CCP) Assured Service

Assessment Criteria for Specialism Recognition

Document History

Version	Date	Notes
1	June 2021	Risk Management Specialism

Contact the NCSC

For general queries and any feedback on this document please contact enquiries@ncsc.gov.uk .

Disclaimer

This document does not replace tailored technical or legal advice on specific systems or issues. NCSC and its advisors accept no liability whatsoever for any expense, liability, loss, claim or proceedings arising from reliance placed on this guidance.

Contents

Introduction

1. This document sets out the assessment process and required evidence for recognition and revalidation in cyber security specialisms under the Certified Cyber Professional (CCP) assured service. The CCP assured service recognises the real-world competence of professionals.

Overview

2. Cyber Security: the National Cyber Security Strategy 2016-2021[1] describes cyber security as 'the protection of information systems (hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm or misuse. This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures'. This document's use of the term 'cyber security' is consistent with that definition. However, it should be recognised that there are many definitions of cyber security and a succinct definition will always be rather abstract. The NCSC is using the Cyber Security Body of Knowledge (CyBOK[2]) to define the discipline of cyber security, including its boundaries, dependencies and relationships with other disciplines.
3. Applicants are expected to be practising cyber security professionals and (in keeping with the standards associated with other NCSC assured services) are required to provide proof of foundational knowledge prerequisites. This proof enables applicants to focus their skill evidence on their proposed specialism. Recognition is based on individuals demonstrating specialist practice in a specific domain (or potentially even domains) of cyber security. It is unlikely, though not impossible, for an individual to demonstrate that they are specialists in more than one domain. There are two levels within the specialisms. The first level is 'Associate Cyber Professional' and the higher level is 'Certified Cyber Professional'.
4. Three Certification Bodies operate the CCP assured service on behalf of the NCSC: APMG[3], BCS, the Chartered Institute for IT[4] and CIISec, the Chartered Institute of Information Security[5]. All follow the same assessment process and criteria. Applications will be assessed using a pass or fail approach.

Guidance for employers and clients of Associate Cyber Professionals and Certified Cyber Professionals

5. Employers and clients are advised that NCSC recognition does not eliminate the need for care in the selection process. Cyber security specialists are not all the same, even within the same specialism. There still needs to be consideration of how relevant an individual's experience, skills and knowledge are to the needs of an organisation. Even if the fit is as close as possible, it may still take some time for them to be fully effective in a new environment.
6. **Associate Cyber Professionals** can apply their expertise in a range of typical risk management circumstances, relating it to the fundamental principles of risk management, for example as an effective and skilled member of a team or within established organisational processes.

---

[1] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

[2] www.cybok.org

[3] https://apmg-international.com/

[4] https://www.bcs.org/

[5] https://www.ciisec.org/

7. The award of **Certified Cyber Professional** aims to identify professionals who are sufficiently versatile to apply their knowledge and skills in a range of organisations, once time has been allowed for absorbing essential differences between different environments.

Application and assessment process

8. Applications may be submitted at any time to one of the three Certification Bodies (APMG, BCS or CIISec). An *example* of the application form is shown at Appendix F. Individuals may choose which Certification Body to apply to - information about each Certification Body can be found on its website, together with an application form for the assessment process. There are two stages in the application process: (1) Demonstration of foundational knowledge; and (2) Assessment of specialist knowledge through case study and interview. Successful applicants must pass both stages.
9. Candidates will usually receive confirmation of the receipt of their application within 10 working days. Notification of whether a case study has met the required threshold will usually be received within 10 working days of case study submission. If the case study is satisfactory, an interview will be arranged. Notification of the overall assessment outcome will usually be provided within 30 - 40 working days after the interview, due to the requirement for moderation to be carried out. Applicants will be informed of any delays to these usual timeframes and the reasons for this.

Foundational knowledge

10. The aim of the NCSC is to ensure that applicants have an approximately commensurate, formally validated and broad level of cyber security knowledge. This can be demonstrated through academic qualifications, professional certifications, professional memberships or proof of NCSC internal skills recognition. The following currently satisfy the requirements for proof of foundational knowledge (this list may be expanded, if additional proposals for inclusion provide a sufficiently broad and formally validated level of cyber security knowledge):
    - An NCSC-certified degree (undergraduate or postgraduate) or
    - A valid certificate for Certified Information Systems Security Professional (CISSP), including full membership of (ISC)² [6] or
    - A valid certificate for Certified Information Security Manager (CISM), including full membership of ISACA[7] or
    - Proof of Full Membership (MCIIS) of the Chartered Institute of Information Security (CIISec) or
    - Proof of having passed an appropriate NCSC internal skills level assessment or
    - Proof of having completed an internal NCSC professional development framework (for example for cyber security architecture).
11. As part of the application process applicants are required to demonstrate evidence of one of the above, typically through the submission of a valid and up-to-date certificate or other proof as appropriate.

[6] https://www.isc2.org/

[7] https://www.isaca.org/

Demonstration of specialist knowledge

12. Applicants select the specialism that they want to be assessed against and create a case study which details the work that they have conducted for customers in the context of that specialism. It is possible for applicants to apply against more than one specialism; however this is unlikely to be commonplace. There must be sufficient evidence of an applicant's practical ability in the professed specialism, therefore up to two case studies may be submitted. All case studies should be supported by customer points of contact who will be contacted. The assessment criteria for case studies follow below (see paragraphs 16-22).
13. If the case study is accepted, applicants will be invited to attend an interview with Certification Body assessors.
14. The case study provides a basis for the interview and applicants are expected to discuss the work they have presented. At the discretion of the assessors, subject matter not included in the case study may also be discussed during the interview, to determine the extent of an applicant's technical knowledge in the claimed specialism and their ability to effectively apply this in a consultative capacity. All interview recommendations will be subject to moderation. Moderation will be performed as necessary but is expected to take place after at least 6 assessments. The interview assessment criteria follow below (see paragraphs 22 – 52 (including the final table)).

Fees

15. All matters relating to certification fees are determined by the Certification Bodies. Information about the cost of certification and how to pay is provided on the Certification Bodies' websites.

Summary of assessment criteria for case study

16. A candidate's case study should demonstrate the relevant criteria for the specialism level for which they are applying. If it is not possible for one case study to cover all the criteria comprehensively, a second case study can be provided. No more than two case studies will be accepted.
17. The referee for each case study will be contacted and must be able to validate and verify the accuracy of the work described. It is expected that the referee's permission for the use of the case study will have been given prior to making the application. If the case study is satisfactory, the candidate will be invited to interview. If the case study is not provided in the way that is required or does not represent good evidence, the Certification Body may provide candidates with information to this effect and may allow one re-submission. If the case study is still unsatisfactory, the Certification Body may fail the application; however, if the resubmitted case study is a borderline fail, assessors should note the areas to explore and ask questions in the interview relevant to the aspects of the case study that need further information, in order to determine whether the applicant has the required degree of specialist knowledge application.
18. **High level requirements**
    - Each case study must not be more than 2 sides of A4 in arial 10-point text size or equivalent. A third side may be added, provided it includes only a diagram and/or a table to support the main document.
    - The case study must cover work carried out within the last 7 years.
    - The case study, its size, value, complexity and strategic importance and the candidate's claimed level of responsibility and role in it must be relevant to the level of risk management specialism for which the candidate is applying.
    - Details of the work completed in the case study should be verifiable.

- All case studies should demonstrate:
    - the candidate's technical abilities through the specialism
    - how the candidate delivered the needs of the client ethically and professionally, making clear their duties/activities
    - how the candidate 'closed the loop' and communicated security and risk effectively to organisations and users

19. Assessors should satisfy themselves that most of the points below are also reflected in the appropriate case study before recommending the applicant should proceed to interview. Justifications, comments and observations can be recorded in the pro forma at Appendix B.

Associate Cyber Professional: additional specific case study criteria

20. It is expected that Associate Cyber Professionals can demonstrate experience working in situations with reasonably complicated risk management scope, but they may do so as an effective and skilled member of a team or within established organisational processes. They can apply their expertise in a range of typical risk management circumstances and can relate it to the fundamental principles of risk management. The case study should reflect that ability and demonstrate:

    1. Business need:
        a. the ability to elicit security requirements that support the overall business need based on straightforward analysis
        b. the ability to directly map between security requirement and business need
        c. clear understanding that security must support organisational priorities and needs
    2. Security direction and governance:
        a. their understanding, support of and participation in enabling organisational cyber security governance
        b. the ability to communicate risk and security concepts effectively in accessible ways that can be clearly understood by business leaders or their delegated representatives
    3. Risk assessment:
        a. sound understanding and evidence of application of the fundamental principles of risk assessment
        b. experience of delivering, or enabling the delivery of, comprehensive risk assessments using suitable risk assessment methodologies in common scenarios with an awareness of the strengths and weaknesses of the chosen approach
        c. the impact of risk realisation is well understood in business terms
        d. understanding the need to take both a top-down view of risk as well as more traditional component-based risk assessment activity
        e. clear explanation of any threat assumptions made and the use of sources of information to illuminate their threat assumptions
        f. the ability to determine and understand the security characteristics of a system to understand actual or potential vulnerabilities
        g. how they 'combine' all the components of risk to arrive at a meaningful assessment and articulation of risk
    4. Risk treatment:

a. understanding of how the output of the risk assessment dovetails into risk treatment and that there is traceability between the most significant identified risks and the measures designed to manage those risks effectively

b. the ability to provide contextualised security advice appropriate to the overall business need delivered with awareness of the sector or environment within which the candidate operates

c. competence and understanding in some technology areas relevant to cyber security in the scenarios or sectors in which they have experience

d. an understanding that risks cannot always be fully mitigated

e. a clear understanding of options such as risk acceptance or transference as well as risk reduction and the role of technical, physical, personnel and procedural controls as a through-life activity

5. Assurance:

a. understanding of the provision of through-life assurance at a service/system as well as component level

b. the ability to apply different assurance approaches with clear understanding of the pros and cons of each

Certified Cyber Professional: additional specific case study criteria

21. Applicants should be demonstrating good experience of all the areas of risk management in the wider and more complex environments in which it is likely they will be engaged. The expectation is that, with limited time necessary to update their business or sector knowledge for a new environment, they could immediately be providing accurate and reliable advice and guidance in any situation with which they are presented. The case study should reflect that ability. The candidate's case study should demonstrate:

1. Business need:

a. the ability to elicit complicated, non-obvious security requirements that are directed by the overall business need

b. the use of different techniques to arrive at an understanding of needs in complicated scenarios

c. the ability to articulate how and why these needs support the overall business aim of the system/service under consideration

2. Security direction and governance:

a. the ability to enable decision makers to make well-informed, balanced and cost-effective risk management decisions in situations with complex scope or significant risk

b. playing a key role in embedding and integrating risk management processes into appropriate corporate governance processes and business activities

c. the ability to communicate difficult risk and security concepts effectively in accessible ways that can be clearly understood by business leaders

3. Risk assessment:

a. an expert understanding and evidence of application of the fundamental principles of risk assessment

b. the ability to deliver, or enable the delivery of, comprehensive risk assessments for complicated or novel scenarios, applying methodologies that are appropriate to the situation, including making adaptations where necessary

c. understanding the need to take both a top-down view of risk as well as more traditional component-based risk assessment activity

d. the impact of risk realisation will be well understood and directly mapped back to business priorities and concerns

e. clear explanation of threat assumptions made and the use of various information sources to illuminate their threat assumptions

f. the ability to determine and understand the security characteristics of a complicated or novel system in order to understand actual or potential vulnerabilities

g. how they 'combine' all of the components of risk in order to arrive at a meaningful assessment and articulation of risk

4. Risk treatment:

   a. a clear understanding of how the output of the risk assessment dovetails into risk treatment and the requirement for clear traceability between the most significant identified risks and the measures designed to manage those risks effectively

   b. the ability to deliver contextualised security advice appropriate to the overall business need including the sociotechnical considerations of the wider system

   c. competence and understanding across a range of technology areas relevant to cyber security whilst drawing upon, using and directing appropriate expertise to solve the bigger security problem

   d. an understanding that risks cannot always be fully mitigated

   e. a clear understanding of the various approaches to addressing risk and the role of technical, physical, personnel and procedural controls as a through-life activity

5. Assurance:

   a. understanding of different approaches to through-life assurance at a service as well as a component level

   b. the ability to combine a range of specific assurance approaches in more complex and unusual situations to provide overall confidence that the things the business values are appropriately protected with clear understanding of the pros and cons of each approach

Summary of assessment criteria for interview

22. Applicants may apply for one or possibly more specialism(s). Each assessment will follow a separate process. The interview focuses on a case study submitted by the applicant. The interview usually lasts approximately 2 hours: whilst interviews will mainly be carried out using an online platform, they can be conducted in person if for reasons of inclusivity that approach is more suitable for a particular applicant. Interviews may be recorded for the purposes of quality checking and for review in case of an appeal against an assessment decision. Certification Bodies reserve the right to share such data with NCSC for the purposes of oversight of the CCP assured service. A transcript will be kept by the Certification Body for legitimate interest in compliance with the UK GDPR[8] and will be destroyed within 6 months of the interview. Certification Bodies are solely responsible for ensuring they comply with all data protection and data storage requirements.

[8] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

23. An applicant's overall technical understanding appropriate to their position as a cyber security professional is assessed, as well as their ability to apply this effectively as a specialist in a consultative capacity. The tables which follow show firstly the criteria for *consultancy skills* and then the criteria for *claimed specialist knowledge*. Both sets of skills are evaluated at the interview.

Consulting skills and behaviours The following consulting skills are a set of behaviours that cyber security professionals will need to exhibit to be effective in their roles as advisors to clients. They are comprised of 3 elements: interviewing and empathy, appropriate style and clear delivery and facilitation.			
Skill	**Fail – bad indicators**	**Pass – Good indicators**	**Comments**
Interviewing and empathy	• Unable to understand or relate to the business needs of a client. • Needs active supervision to ensure the client's business priorities, technical context and timescales are fully explored.	• Engages effectively with the client to understand needs and drivers. • Understands the business context and the agenda of the stakeholders. • Balance of talking and listening (70 – 30). • Concerned and inquisitive.	
Clear delivery and appropriate style	• Does not organise arguments well and tends to mix key issues with trivia. • Finds it difficult to adapt style to different levels of audience. • Tendency to ramble and describe too much detail. • May interrupt the speaker.	• Presents arguments in a clear and articulate manner selecting the appropriate level of detail to suit the audience. • Good eye contact. • Effective time management.	
Facilitation	• Unable to take an independent position. • Unable to ensure that all voices are heard. • Likely to find it difficult to manage conflicts.	• Can build consensus, manage conflict and achieve conciliation, and offer arbitration. • Keen to come to an acceptable conclusion. • Keen to ensure that all parties understand the other party's point of view.	
Summary of overall indicators	• Arrogance • Pomposity • Grandiose • Lack of interest	• Natural/comfortable in demeanour • Confident • Respectful	

Table 1: Consultancy Skills (Associate Cyber Professional and Certified Cyber Professional)

Associate Cyber Professional interview: specialist knowledge assessment criteria (risk management specialism)

24. The interview focuses on the submitted case study and assesses the applicant's overall technical understanding appropriate to their position as a cyber security professional. The interview usually requires approximately 2 hours and, like the case study, is divided into 5 distinct risk management sections:

- establishing business need
- establishing the security direction and governance
- the approach to risk assessment
- the approach to treatment
- the assurance approach

25. Some sample questions may be used as prompts for a conversation but are not mandatory. Assessors will use their judgement as to the questions that allow an applicant to best express their risk management experience. There are no trick questions and the applicant should ask for clarification if a question is not clear or they need it to be repeated.

26. Pass and fail indicators are provided to assist with the assessment. There is an overall expectation that pass indicators will predominate, although a few fail indicators are acceptable. Additional indicators can be considered, as the list provided is not exhaustive. The assessor's judgement is paramount.

27. The assessment documentation should include comments to support the decisions and recommendations made. These will also be used for feedback and moderation. Any additional observations or recommendations for the applicant should also be recorded. Assessors seek to understand whether the applicant has a sound grasp of technology and its cyber security implications. Deep expertise is not expected but applicants should show enough technical understanding to be credible across a range of core technologies. The assessment process focuses on the broad technical disciplines in the case studies, with additional questions aimed at understanding breadth of technical understanding.

Establishing business need

28. The applicant can elicit security requirements, based on straightforward analysis, that support the overall business need. There should be an ability to directly map between security requirements and business need and to demonstrate that they understand that security must support organisational priorities and needs. There should be evidence of use of some techniques to arrive at an understanding of a security need, such as threat tree analysis or use of security principles-based derivation.

Security direction and governance

29. Applicants need to show that they clearly understand, support and participate in enabling organisational cyber security governance: this can be working within the constraints of existing governance arrangements.

30. They clearly understand who the business decision-makers are and provide them with sufficient and appropriate information to help them make well-informed, balanced and cost-effective risk management decisions throughout the lifecycle of a service or system. Provision of information to decision-makers can be via established organisational structures and processes, but the applicant should understand how those processes support decision making. They understand and support the embedding and integration of risk management processes into appropriate corporate governance processes and business activities.

31. They can communicate risk and security concepts effectively in accessible ways that can be clearly understood by business leaders or their delegated representatives. Equally the applicant is expected to demonstrate an ability to understand business direction and intent such as described in risk appetite statements. Evidence should show the interpretation of such statements into meaningful and appropriate security requirements or guidance that can be applied by others.

Risk assessment

32. Applicants must demonstrate sound understanding and evidence of using fundamental principles of risk assessment and experience of delivering, or enabling the delivery of, comprehensive risk assessments in common scenarios. They understand, adapt and apply suitable risk assessment methodologies with an awareness of the strengths and weaknesses of the chosen approach. An applicant must also demonstrate an appropriate top-down view of risk as well as being able to undertake more traditional component-based risk assessment activity meaningfully.

33. The impact of risk realisation will be well understood in business terms. An applicant will be able to explain clearly any threat assumptions made and the use of sources of information to explain their threat assumptions. They should show how they determine and understand the security characteristics of a system in order to understand actual or potential vulnerabilities and explain how they 'combine' all the risk components to arrive at a meaningful assessment and articulation of risk.

Risk treatment

34. The applicant can understand and describe clearly how the output of the risk assessment dovetails into risk treatment and that there is traceability between the most significant identified risks and the measures designed to manage those risks effectively. Where frameworks are used (either organisational control frameworks or published standards) there is clarity about what risks these mitigate and what they do not.

35. Security advice is contextualised and appropriate to the overall business need. It is delivered with awareness of the sector or environment within which the applicant operates. They can recognise (and minimise) when security measures might impact users or the business and can provide information to help decision makers take well informed decisions.

36. The applicant can demonstrate competence and understanding in some technology areas relevant to cyber security in the scenarios or sectors in which they have experience. They may demonstrate calling upon additional experts to technically support their risk management processes. The applicant understands options such as risk acceptance or transference as well as risk reduction. Risk mitigation strategies draw from and recognise all physical, personnel and procedural controls as well as the technical. They understand that risks cannot always be fully mitigated and are mindful of the role of designing to minimise the impact of compromise, coupled with steps to easily detect and respond to incidents. Risk treatment is considered as a through-life activity that requires attention at service design and through the entire service/system lifecycle. Evidence will extend beyond purely protective measures and include, for example, detection of security issues (monitoring) and incident response.

Assurance

37. The applicant understands and can describe provision of assurance for the system or service under consideration. This includes assurance at a service/system as well as component level and is applicable at all stages of the lifecycle of the service or system. They understand and apply different approaches to (for example) product, implementation/architectural and operational assurance. There is clear understanding of the pros and cons of different assurance activities.

1. Establish the business need (10 to 15 minutes)				
Pass indicators	**Fail indicators**	**Sample questions**	**Pass/Fail**	**Comments**
1. Evidence of how business needs are gathered and understood, including an understanding of high-level business objectives.	1. Focusses on simple C, I and A (Confidentiality, Integrity and Availability) requirements without business context.	[explore the process of establishing security requirements based upon business need in the provided case study] Describe a situation where you helped a		

1. Establish the business need (10 to 15 minutes)				
Pass indicators	**Fail indicators**	**Sample questions**	**Pass/Fail**	**Comments**
2. Can clearly demonstrate elicitation of straightforward security needs. 3. Understands and can articulate how security requirements directly support the needs of the business. 4. Demonstrates an ability to help an organisation understand their security needs as necessary to support their business objectives. 5. Demonstrates an understanding and ability to balance business objectives and security needs. 6. Can explain how they identify key stakeholders (or their representatives) from within the business and understand their priorities and concerns.	2. Determines business need from just a regulatory or compliance basis. 3. Security does not support and is not mapped to business need or objective. 4. Lack of evidence that the business was appropriately consulted or considered. 5. Unable to demonstrate the ability to map or explain security requirements in business terms.	customer understand and articulate their security needs. 1. How did you approach this? 2. What did you do? 3. What was the outcome? Describe a situation where there was an actual or perceived conflict between security requirements and business need. 1. How was the conflict identified? 2. What was your approach to resolving the conflict? 3. What was the outcome?		

2. Security direction and governance (10 to 15 minutes)				
Pass indicators	**Fail indicators**	**Sample questions**	**Pass/Fail**	**Comments**
1. Clearly understands and has evidence of participating within organisational governance mechanisms. 2. Can identify who the real decision-makers are with responsibility for the service or system within the scope of the analysis and understands how security impacts upon their responsibilities. 3. A demonstrated ability to articulate security concepts to business leaders or their representatives which helps them to make well informed decisions. 4. Can understand and interpret decision-makers' risk appetite statements and tolerances with regards to things that are important. There is some evidence of being able to turn that top-level intent into meaningful security direction. 5. Aware of applicable legislation, regulation and/or standards and the implications in the context under consideration.	1. Does not understand governance structures and decision-making in the organisations within the scope of the assessment. 2. Cannot explain risk appetite in a meaningful way or explain how it could be interpreted in the context of the case study. 3. Unable to demonstrate how they work with business direction such as risk appetite and tolerance statements in a meaningful manner. For example, talking about risk appetite in an entirely abstract sense (averse – hungry). 4. A lack of understanding about applicable legislation, regulation and/or standards.	Tell me how governance was approached when you worked with [case study]. 1. What was your role and how did you support the governance arrangements? 2. How did you work within these arrangements? How was risk appetite articulated? 3. How did this shape/direct subsequent risk management activities? How were security decisions made? 4. What was your role in supporting or informing those decisions? Were there any legal, regulatory or policy considerations that influenced how security governance and decision making worked? Can you give me an example of where you believed the wrong security decision was made? 5. Why did you believe this was the case? 6. What did you do?		

3. Risk assessment (40 to 45 minutes)				
Pass indicators	**Fail indicators**	**Sample questions**	**Pass/Fail**	**Comments**
1. Can describe application of the fundamental principles of risk assessment to situations of reasonably complex scope. 2. Recognises the need for, benefits and limitations of different types of risk assessment approaches. They can explain a rationale for methods they have used including how they may have modified the method to best suit their context. 3. Can clearly explain how they determine applicable business assets/things of value and the impact to these assets should they be affected or compromised. They undertake this in conjunction with key stakeholders. 4. Clearly explains how they determine an applicable threat model, the vulnerabilities that could be exploited and how this could impact the identified assets. 5. Recognises the limitations of their risk analysis, for example determination of threat motivation or reputational impact. 6. Understands the applicability, benefits and limitations of qualitative versus quantitative analysis methods.	1. The risk assessment approach is process-driven ('turn handle') and shows little flexibility or customisation. There is a lack of understanding of how methods or approaches support fundamental risk assessment principles. 2. The assessment approach is immature and there is a poor understanding of the relationship between the constituent parts of the assessment. 3. The approach to analysis is inflexible with a preference for applying one approach to all aspects of risk assessment. 4. Refers to impact assessment in an abstract sense, such as simply by reference to classification. 5. The understanding of threat is immature, and sources of threat information are used without understanding or contextualization. 6. Risk assessments are conducted in isolation of the business objective. 7. Qualitative and quantitative approaches are confused and not used appropriately. 8. A process only based approach to presentation and prioritisation is followed, for example by combining abstract criteria using a matrix. 9. Risks are prioritised and presented in the same way irrespective of the audience.	Talk through the approach to risk assessment when you worked with [case study] 1. Did you work with a specific risk assessment method? 2. Why did you choose to work with that method? 3. What modifications did you need to make for your situation? How did you identify the scope of the assessment and how did this determine the approach taken? Can you explain your approach to identifying key assets? 4. What was identified and why? 5. What did the business care about and why? How did you determine the applicability of relevant sources of threat? 6. How did you validate your threat model? 7. What technical assumptions did you make about the identified threat? How did you assess vulnerability in the system or service under consideration? 8. What approaches did you use to support your analysis?		

3. Risk assessment (40 to 45 minutes)				
Pass indicators	**Fail indicators**	**Sample questions**	**Pass/Fail**	**Comments**
7. Risk assessment output is well constructed, meaningful and tailored to the audience needs. Risks are well contextualised to aid decision making. 8. Able to explain and justify the approach to prioritisation of risks by comparing and balancing different types of risk from across the organisation.	10. Risks are presented and prioritised in a biased way so that the audience is drawn to improbable or unrealistic risks. 11. Risks are dismissed and/or prioritised only according to the views of the applicant – there is little indication that the business has been consulted.	How did you gain confidence in your analysis? Talk us through the approach to evaluating, presenting and prioritising the risks you identified for [case study] 9. Can you describe the rationale behind the risks that you had identified and the corresponding severity? 10. Of the risks identified, how did you determine which ones should be prioritised? 11. How do you differentiate between high impact/low probability and low impact/high probability? Other than security stakeholders, were there any other parts of the business that you shared your findings with? 12. How did you ensure they understood the risk presentation? How was the risk assessment received by the business? 13. Were there any challenges to what you presented? In the context of existing answers above what were the top 3 risks identified?		

4. Risk treatment (25 to 30 minutes)				
Pass indicators	**Fail indicators**	**Sample questions**	**Pass/Fail**	**Comments**
1. Able to articulate evidence of developing risk mitigation strategies that manage specific and defined high magnitude risks. 2. Can describe the creation of risk mitigation strategies to mitigate classes of risks (such as risks arising from 'commodity' internet-based attacks). 3. Demonstrates an ability to understand when and how to use control frameworks appropriately and the classes of risks that can be managed by these. 4. Mindful of different risk treatment options (treat, transfer, accept etc.) and uses organisational direction to influence recommended treatment options. 5. Recognises the limitations of risk mitigation approaches and the need to manage residual risk appropriately. 6. Understands and can demonstrate the need for holistic mitigation based on physical, personnel, procedural and technical control types. 7. Understands that systems change (for example, operational need changes, threat changes or emergent vulnerabilities), so management needs to be ongoing.	1. Risk treatment is described in isolation from the business, without empowering the business decision maker regarding treatment options. 2. Unclear how recommended controls actually mitigate the identified risks whilst supporting the business need. 3. Risk mitigation tends to be dominated by the use of standard control frameworks and they're unclear when that may not be appropriate. 4. The approach to risk treatment is based solely upon compliance, rather than management of actual risk. 5. Does not recognise when security measures might impact users or business needs. 6. Unable to provide security advice in a contextual manner appropriate to the circumstances in which they are working. 7. Risk treatment is considered only at a single point of time (such as an accreditation milestone) rather than throughout the whole lifecycle.	Talk through the approach to managing the top 3 identified risks for [case study] 1. How did you decide and agree upon the suitability of the controls? 2. How did you ensure that the approach will remain effective throughout the system lifecycle? How did you ensure traceability between the assessed risks and the subsequent mitigation activities? Did you work with any control sets to support treatment? 3. If so, how did you work with them? 4. What were the pros and cons of those control sets? Can you give me an example of where you were asked to justify a specific mitigation to the business? Were there any situations where it was not possible to mitigate a risk? 5. If so, what did you do? How were residual risks identified and how were these managed? Can you describe a situation where you were		

4. Risk treatment (25 to 30 minutes)				
Pass indicators	**Fail indicators**	**Sample questions**	**Pass/Fail**	**Comments**
8. Understands when security measures might impact on users or business needs and is able to provide effective advice to help the business make appropriate decisions. 9. Delivers security advice that is contextualised and appropriate for the customer need. Avoids providing 'point' solutions or advice that does not address the overall key security issues.		required to explain a complex security recommendation to a senior person who did not have the time or technical knowledge to understand the problem? • What approach did you take? • Was the person able to make an informed judgement? Describe a situation when you have provided advice to defend against a potential future risk rather than a visible current one. Sample technical questions may also be asked, examples of which can be found at Appendix I.		

5. The assurance approach – 15 – 20 minutes				
Pass indicators	**Fail indicators**	**Sample questions**	**Pass/Fail**	**Comments**
1. Understands different sources and approaches for gaining assurance. This includes a clear understanding of the benefits and limitations of different assurance techniques. 2. Applies a range of assurance approaches to solutions, with a clear understanding of the strengths and limitations of each approach.	1. There is little awareness of the need for assurance. 2. The approach to assurance is driven solely by compliance with artefacts such as classification. 3. There is evidence of a dogmatic approach to assurance for example mandating certified products without clear reasoning.	Talk through the approach to assurance for [case study] Can you provide some examples of assurance activities and explain the pros and cons of them? How did you demonstrate confidence to a business leader or their representative that their overall concerns were appropriately protected?		

5. The assurance approach – 15 – 20 minutes				
Pass indicators	**Fail indicators**	**Sample questions**	**Pass/Fail**	**Comments**
3. Assurance and confidence are not limited to a point in time, but the applicant seeks to address confidence across the system/service lifecycle. 4. Understands and applies different approaches to product, implementation and operational assurance. Uses each appropriately to derive a genuine understanding of confidence that the overall business objective is protected.	4. The applicant focuses on specific aspects of assurance activity rather than determining overall confidence at a system level. 5. Assurance is conducted at a single point in time rather than across the lifecycle of the system/service. 6. Cannot explain how different approaches to products, implementation and operational assurance can be effective.	Can you give an example of where you have had to provide confidence that risks will remain managed through system life?		

Table 2: Associate Cyber Professional (application of specialist knowledge interview)

Certified Cyber Professional interview: specialist knowledge assessment criteria (risk management specialism)

38. The interview focuses on the submitted case study/ies and assesses the applicant's overall technical understanding appropriate to their position as a cyber security professional. The interview usually requires approximately 2 hours and, like the case study, is divided into 5 distinct risk management sections:
    - establishing business need
    - establishing the security direction and governance
    - the approach to risk assessment
    - the approach to treatment
    - the assurance approach
39. The interview is based on a conversation about the applicant's work on the submitted case study. Some sample questions are provided, which can be used as prompts for a conversation but are not mandatory. The assessor should use their judgement as to the questions that allow the applicant to best express their risk management experience. There are no trick questions and the applicant should be told to ask for clarification if a question is not clear or they need it to be repeated.
40. Pass/fail indicators are used by the assessor to moderate and gauge the answers given. There is an overall expectation that the applicant will mostly demonstrate pass indicators for each section. A few fail indicators are acceptable but should not dominate. For either pass or fail the assessor's judgement is paramount and the indicators should not be taken as a check list.

41. The comments area on the assessment sheet should be used to record and justify decisions. This will help with feedback as well as enable cross applicant moderation activities. Any additional observations or recommendations for the applicant should also be recorded. Assessors seek to understand whether the applicant has a good grasp of technology and the consequent cyber security implications. Whilst not looking for deep expertise, there should be enough technical understanding to make the applicant credible across a range of core technologies. The assessment process follows the broad technical disciplines applicable to the described case studies, with a few additional questions aimed at understanding breadth of technical understanding.

42. It is expected that Certified Cyber Professionals will demonstrate a range of experience and work on situations with complicated risk management scope. They will be able to apply their expertise in difficult or unusual circumstances with no clear precedent, based on the application of the fundamental principles of risk management.

Establishing business need

43. The applicant can elicit complicated, non-obvious security requirements that are directed by the overall business need. The mapping between business need, the technology that supports that need and how it might be impacted may be non-trivial to deduce. They should be able to demonstrate the use of different techniques to arrive at an understanding of needs in complicated scenarios. This might include methods such as threat tree analysis, security principles-based derivation or other more formal engineering techniques. They will clearly be able to articulate how and why these needs support the overall business aim of the system/service under consideration.

Security direction and governance

44. The applicant plays a key role in enabling organisational cyber security governance. They put in place steps to enable decision makers to make well informed, balanced and cost-effective risk management decisions on situations with complex scope or significant risk. They play a key role in embedding and integrating risk management processes into appropriate corporate governance processes and business activities. Business decision making is supported by the development of approaches to communicate effectively and report on security risk (both at design and throughout a system's lifecycle) to those responsible for making risk-based decisions for a given system or capability. They can communicate difficult risk and security concepts effectively in accessible ways that can be clearly understood by business leaders. Equally the applicant is expected to demonstrate an ability to help decision makers express their security intent (such as expressed risk appetite statements) in ways that can be interpreted by others, such as technical architects or service developers.

Risk assessment

45. The applicant will have expert understanding and evidence of application of the fundamental principles of risk assessment. They will have experience of delivering, or enabling the delivery of, comprehensive risk assessments for complicated or novel scenarios. They will understand and apply methodologies that are appropriate to the situation, including making adaptations where necessary. They will understand the need to take both a top-down view of risk as well as being able to undertake meaningfully more traditional component-based risk assessment activity.

46. The impact of risk realisation will be well understood and directly mapped back to business priorities and concerns. The applicant will be able to explain clearly threat assumptions made and will use various sources of information to illuminate their threat assumptions. There will be evidence of being able to determine and understand the security characteristics of a complicated or novel system to understand actual or potential vulnerabilities. They will be able to explain how they combine all the components of risk to arrive at a meaningful assessment and articulation of risk.

Risk treatment

47. The applicant can understand and describe clearly how the output of the risk assessment dovetails into risk treatment and that there is clear traceability between the most significant identified risks and the measures designed to manage those risks effectively. Where frameworks are used (either organisational control frameworks or published standards) there is clarity about what classes or risks these mitigate and what they do not. They are used appropriately.

48. Security advice is contextualised and appropriate to the overall business need. The applicant will avoid providing 'point' solutions to a narrow risk that does not address the overall key business needs. They will look at the wider 'system' which includes sociotechnical considerations (such as the role the user plays in meeting the desired security outcome). Security advice will be appropriate for the development model the customer is following. This might include things such as security in a complicated supply chain through to security in a Continuous Integration/Continuous Delivery (CI/CD) environment.

49. The applicant will have demonstrated competence and understanding across a range of technology areas relevant to cyber security. This is not about being an expert in everything but having enough awareness and understanding to be credible across the technical discipline. In addition, where the applicant provides security advice that goes beyond their personal expertise, they will be able to demonstrate drawing upon, using and directing appropriate expertise to solve the bigger security problem.

50. The applicant understands options such as risk acceptance or transference as well as risk reduction and can describe the role of those options in their evidence. Risk mitigation strategies draw from and recognise all physical, personnel and procedural controls as well as the technical. They understand that risks cannot always be fully mitigated and are mindful of the role of designing to minimise impact of compromise coupled with steps to easily detect and respond to incidents.

51. Risk treatment is considered as a through-life activity that requires attention at service design and through the entire service/system lifecycle. Evidence will extend beyond purely protective measures and include, for example, detection of security issues (monitoring) and incident response.

Assurance

52. The applicant clearly understands and can describe provision of assurance for the system or service under consideration. This includes assurance at a service as well as a component level and is applicable at all stages of the lifecycle of the service or system. They understand and apply different approaches to (for example) product, implementation/architectural and operational assurance. There is clear understanding of the pros and cons of different assurance activities. The applicant can combine a range of specific assurance approaches to provide overall confidence that the things the business values are appropriately protected.

1. Establish the business need (10 to 15 minutes)				
Pass indicators	**Fail indicators**	**Sample questions**	**Pass/Fail**	**Comments**
1. Evidence of how business needs are systematically determined, gathered and understood, including an understanding of high-level mission objectives.	1. Focusses on simple C, I and A (Confidentiality, Integrity and Availability) requirements without business context. 2. Determines business need from just a regulatory or compliance basis.	[explore the process of establishing security requirements based upon business need in the provided case study] Describe a situation where the customer was unable to clearly articulate their security requirements 1. How did you approach this?		

1. Establish the business need (10 to 15 minutes)				
Pass indicators	**Fail indicators**	**Sample questions**	**Pass/Fail**	**Comments**
2. Understands and uses appropriate methods and techniques for establishing business need. 3. Can demonstrate elicitation of complicated, non-obvious security needs. For example, where the mapping between business need, the technology that supports that need and how it might be impacted is non-trivial to deduce. 4. Understands and can articulate how security requirements directly support the needs of the business. 5. Demonstrates an ability to help an organisation reason about their security needs as necessary to support their business objectives. 6. Demonstrates an understanding and ability to balance what may appear to be competing needs between business objectives and security. 7. Can explain how they identify key stakeholders from within the business and determination of their priorities and concerns.	3. Security does not support and is not clearly mapped to business need or objective. 4. Lack of evidence that the business was effectively consulted or considered. 5. Did not provide evidence of adapting the service offering in response to business needs. 6. Shows a lack of understanding of standardised ways of determining security requirements. 7. Unable to demonstrate the ability to map or explain complicated security requirements.	2. What did you do? 3. What was the outcome? Describe a situation where there was an actual or perceived conflict between security requirements and business need 1. How was the conflict identified? 2. What was your approach to resolving the conflict? 3. What was the outcome? Describe a situation where the customer didn't agree with your assessment of security need. 1. What was the basis of the disagreement? 2. How did you respond? 3. Were you able to come to an agreement?		

2. Security direction and governance (10 to 15 minutes)				
Pass indicators	**Fail indicators**	**Sample questions**	**Pass/Fail**	**Comments**
1. Clearly understands and has evidence of shaping organisational governance mechanisms. This may include establishing new, effective, governance mechanisms or demonstrating expert use of more complex existing processes to support a given project or system. 2. Can identify who the real decision makers are with responsibility for the service or system within the scope of the analysis and help them understand how security impacts upon their responsibilities. 3. A demonstrated ability to articulate complex security concepts to business leaders and decision makers which enables them to make well informed decisions. 4. Helps decision-makers deduce their risk appetite and tolerances with regards to things that are important to them. There is evidence of being able to turn top-level intent into meaningful direction for others. 5. Aware of applicable legislation, regulation and/or standards and the implications in the context under consideration.	1. Does not clearly understand governance structures and decision making in complex organisations or situations. 2. Can only demonstrate an ability to work within established and well-defined existing governance structures. 3. Cannot explain risk appetite in a meaningful way or explain how it could be interpreted in the context of the case study. 4. Unable to demonstrate how they work with decision makers to understand and deduce risk appetite and tolerances in a meaningful manner. For example, talking about risk appetite in an abstract sense (averse – hungry). 5. A lack of understanding about applicable legislation, regulation and/or standards.	Tell me how governance was approached when you worked with [case study] 1. What was your role in establishing governance arrangements? 2. How did you work within these arrangements? How was risk appetite determined and articulated? 3. How did this shape/direct subsequent risk management activities? How were security decisions made? 4. What was your role in supporting or informing those decisions? Were there any legal, regulatory or policy considerations that influenced how security governance and decision making worked? Can you give me an example of where you believed the wrong security decision was made? 5. Why did you believe this was the case? 6. What did you do?		

3. Risk assessment (40 to 45 minutes)				
Pass indicators	**Fail indicators**	**Sample questions**	**Pass/Fail**	**Comments**
1. Can describe application of the fundamental principles of risk assessment to situations of significantly complex scope. 2. Recognises the need for, benefits and limitations of different types of risk assessment approaches. They can explain a rationale for methods they have used including how they may have modified the method to best suit their context. 3. Can clearly explain how they determine applicable business assets/things of value and the impact to these assets should they be affected or compromised. They undertake this in conjunction with key stakeholders. 4. Clearly explains in detail how they determine an applicable threat model, the vulnerabilities that could be exploited and how this could impact the identified assets. 5. Recognises the limitations of risk analysis, for example determination of threat motivation, reputational impact or complex system dynamics. 6. Understands the applicability, benefits and limitations of qualitative versus quantitative analysis. 7. Risk assessment output is well constructed, meaningful and tailored to the audience needs. Risks are well contextualised to aid decision making.	1. The risk assessment approach is process-driven ('turn handle') and shows little flexibility or customisation. There is a lack of understanding of how methods or approaches support fundamental risk assessment principles. 2. The assessment approach is immature and there is a poor understanding of the relationship between the constituent parts of the assessment. 3. The approach to analysis is inflexible with a preference for applying one approach to all aspects of risk assessment. 4. Refers to impact assessment in an abstract sense, such as simply by reference to classification. 5. The understanding of threat is immature, and sources of threat information are used without deep understanding and contextualization. 6. Risk assessments are conducted in isolation of the business objective. 7. Qualitative and quantitative approaches are confused and not used appropriately. 8. Only process based approach to presentation and prioritisation are followed, for example by combining abstract criteria using a matrix.	Talk through the approach to risk assessment when you worked with [case study] 1. Did you work with a specific risk assessment method? 2. Why did you choose to work with that method? 3. What modifications did you need to make for your situation? How did you identify the scope of the assessment and how did this determine the approach taken? Can you explain your approach to identifying key assets, what these were and why? 4. What did the business care about and why? How did you determine the applicability of relevant sources of threat? 5. How did you validate your threat model? 6. What technical assumptions did you make about the identified threat? How did you assess vulnerability in the system or service under consideration? 7. What approaches did you use to support your analysis?		

3. Risk assessment (40 to 45 minutes)				
Pass indicators	**Fail indicators**	**Sample questions**	**Pass/Fail**	**Comments**
8. Able to explain and justify the approach to prioritisation of risks by comparing and balancing different types of risk from across the organisation.	9. Risks are prioritised and presented in the same way irrespective of the audience. 10. Risks are presented and prioritised in a biased way so that the audience is drawn to improbable or unrealistic risks. 11. Risks are dismissed and/or prioritised only according to the views of the applicant.	How did you gain confidence in aspects of your analysis? Talk us through the approach to evaluating, presenting and prioritising the risks you identified for [case study] 8. Can you describe the rationale behind the risks that you had identified and the corresponding severity? 9. Of the risks identified, how did you determine which ones should be prioritised? 10. How do you differentiate between high impact/low probability and low impact/high probability? How was the risk assessment received by the business? 11. Were there any challenges to what you presented? In the context of existing answers above what were the top 3 risks identified?		

4. Risk treatment (25 to 30 minutes).				
Pass indicators	**Fail indicators**	**Sample questions**	**Pass/Fail**	**Comments**
1. Able to articulate evidence of developing risk mitigation strategies that manage specific and defined high magnitude risks. 2. Can describe the creation of risk mitigation strategies to mitigate classes of risks (such as risks arising from 'commodity' internet-based attacks). 3. Demonstrates an ability to understand when and how to use control frameworks appropriately and the classes of risks that can be managed by such. 4. Mindful of different risk treatment options (treat, transfer, accept etc) and uses organisational direction to influence recommended treatment options. 5. Recognises the limitations of risk mitigation approaches and the need to manage residual risk appropriately. 6. Understands and can demonstrate the need for holistic mitigation based on physical, personnel, procedural and technical control types. 7. Understands that systems change (for example, operational need changes, threat changes or emergent vulnerabilities), so management needs to be ongoing.	1. Risk treatment is described in isolation from the business, without empowering the business decision maker regarding treatment options. 2. Unclear how recommended controls would actually mitigate the identified risks so as to support business needs. 3. Only able to explain the use of standard control frameworks and unclear when that may not be appropriate. 4. The approach to risk treatment is based solely upon compliance, rather than management of actual risk. 5. Does not recognise when security measures might impact users or business needs. 6. Unable to provide security advice in a contextual manner appropriate to the circumstances in which they are working. 7. Security advice is limited and does not go beyond standard approaches. 8. Risk treatment is considered only at a single point of time (such as an accreditation milestone) rather than throughout the whole lifecycle.	Talk through the approach to managing the top 3 identified risks for [case study] 1. How did you decide and agree upon the suitability of the controls? 2. How did you ensure that the approach will remain effective throughout the system lifecycle? How did you ensure traceability between the assessed risks and the subsequent mitigation activities? Did you work with any control sets to support treatment? 3. If so, how did you work with them? Can you give me an example of where you were asked to justify a specific mitigation to the business? Were there any situations where it was not possible to mitigate a risk? 4. If so, what did you do? How were residual risks identified and how were these managed? Can you describe a situation where you were required to explain a		

4. Risk treatment (25 to 30 minutes).				
Pass indicators	**Fail indicators**	**Sample questions**	**Pass/Fail**	**Comments**
8. Understands when security measures might impact on users or business need and is able to provide effective advice to help the business make appropriate decisions. 9. Delivers security advice that is contextualised and appropriate for the overall need. The applicant avoids providing 'point' solutions or advice that does not address the overall key business security needs. 10. Looks at the wider 'system' which includes sociotechnical considerations (e.g., the role the user plays in meeting the desired security outcomes). 11. Security advice offered by the applicant extends beyond particular technologies with which the applicant is familiar and draws upon and directs appropriate expertise. 12. Security advice is appropriate for the development model the customer is following. This might include things such as security in a complicated supply chain through to security in CI/CD environments.		complex security recommendation to a senior person who did not have the time or technical knowledge to understand the problem. • What approach did you take? • Was the person able to make an informed judgement? Have you dealt with a customer who had a preconceived idea of what the solution should be and you have had to influence their perception? • How did you approach this? • How did you go about getting them to be open to other ideas? • Did they change their position? Describe a situation when you have provided advice to defend against a potential future risk rather than a visible current one Sample technical questions may also be asked, examples of which can be found at Appendix I.		

5. The assurance approach (15 – 20 minutes)				
Pass indicators	**Fail indicators**	**Sample questions**	**Pass/Fail**	**Comments**
1. Understands different sources and approaches to gaining assurance. This includes a clear understanding of the benefits and limitations of different assurance techniques. 2. Applies a range of assurance approaches to solutions, with a clear understanding of the strengths and limitations of each approach. There is a clear ability to map the assurance options recommended directly to the security need to be addressed. 3. Assurance and confidence are not limited to a point in time but the applicant seeks to address confidence across the system/service lifecycle. 4. The applicant understands and applies different approaches to product, implementation and operational assurance. Uses each appropriately to derive a genuine understanding of confidence that the overall business objective is protected.	1. There is little awareness of the need for the assurance. 2. The approach to assurance is driven solely by compliance or artefacts such as classification. 3. There is evidence of a dogmatic approach to assurance for example mandating certified products without context. 4. The applicant focuses on specific aspects of assurance activity rather than determining overall confidence at a system level. 5. Assurance is conducted at a single point in time rather than across the lifecycle of the system/service. 6. Cannot explain how different approaches to products, implementation and operational assurance can be effective.	Talk through the approach to assurance for [case study] How did you demonstrate confidence to a business leader that their overall concerns were appropriately protected? Can you give an example of where you have had to provide confidence that risks will remain managed through system life? Can you provide some examples of assurance activities and explain what the value of these were? How did you work with the risk appetite to gauge appropriate assurance?		

Table 3: Certified Cyber Professional (application of specialist knowledge interview)

Feedback

53. In the event that recognition in the specialism is not awarded, information will be provided about the reasons for this. Applicants may re-apply at their own cost, however no more than 3 applications in total for the same specialism should be made in any 12-month period.

Revalidation process

54. The goal of the revalidation process is to ensure that all specialists maintain a good level of current knowledge and proficiency in their cyber security practice. This should enhance their ability to manage, design, oversee, assess or advise on the cyber security of systems, as appropriate. Revalidation is required every 18 months following the initial award of recognition in a CCP specialism.

55. A log of continuing professional development (CPD) and continuing professional education (CPE) is required for each year of practice. Specialists who already complete CPD/CPE evidence as part of their CISSP certification and membership of (ISC)², or CISM certification and membership of ISACA, or as part of their membership of CIISec should provide a copy of that CPD/CPE evidence to their CCP Certification Body in order to be assessed for revalidation.

56. Specialists who are not members of (ISC)², ISACA or CIISec should complete the template log at Appendix G, stating the nature of their CPD/CPE activity, its benefits and the impact it has had on their work. The requirement is for 120 hours of CPD/CPE over a total of 3 years, with a minimum of 20 hours each year. This is in keeping with the CPD/CPE requirements of those professional membership bodies. By way of example only, activities may include:

    - completing an educational course in cyber security[9]
    - reading an article or book on cyber security
    - publishing a book, whitepaper or article on cyber security
    - attending a conference (in-person or virtual), educational course, seminar or presentation about cyber security
    - completing a presentation or similar related to cyber security
    - work on cyber security which is not part of normal work duties
    - researching a cyber security issue or preparation for a cyber security certification or undertaking a higher education course in cyber security[9]
    - volunteering/pro bono cyber security work for government, public sector and charitable organisations

57. In all cases, assessors reserve the right to request further evidence if required (exceptionally this might take the form of an interview). Any requirement for further evidence should be fully justified with a clear explanation of why it is needed.

[9] If attendance on training or educational courses is provided as part of this evidence, it needs to be clear how the knowledge and skills acquired in this way are being applied in practice.

Appendix A: Exemplar case studies

Associate Cyber Professional sample case study: Critical National Infrastructure operator of essential services

We were approached in early 2017 to provide a small team, including me as the Chief Security Officer (CSO), for a minimum 6-month period to support an international Managed Service Provider's (MSP) $120 million contract with a multinational energy company. The Energy Company had been classified as an Operator of Essential Services (OES) under the NIS Directive and therefore needed to show its Competent Authorities, Ofgem, HSE and the Department for Business, Energy & Industrial Strategy (BEIS), that it met its security obligations.

With an annual turnover of £74 billion, the OES produces and distributes oil and gas 24/7/365 in 15 countries, including the UK, Europe and the USA. It was part way through planning a major mid-life refresh of its mainly on-prem corporate network, with a significant part of the tech refresh being migration to hybrid-cloud. The MSP were under considerable contractual pressure to deliver the mid-life refresh, securely, on time and on budget with significant commercial penalties for failure. The oil and gas production environments were logically and physically divorced from the corporate network and out of scope for the tech refresh.

The combined OES and MSP team numbered about 900, with the majority based at the UK corporate HQ, approximately 620 of them provided by the MSP. These included the 15 remaining members of the Information Assurance and Security Team, directed and managed by the CSO. The latter is a Board Level appointment responsible to the MSP's General Manager for the secure operation of the OES's corporate networks; physical security of the HQ Building; personnel security for all MSP staff on the team; auditing and monitoring through the on-site SOC; secure architecture in design and operation of the corporate infrastructure and all associated applications wherever they are accessed; the annual assurance programme; security incident management and external liaison with HSE, Ofgem and BEIS.

On speaking to senior stakeholders from both the OES and the MSP about their Risk Appetite, I identified significant concern about the level of cyber related risk to which the OES corporate network was exposed.

The MSP could absolutely not afford the refresh project to fail, the OES was adamant that nothing be allowed to impact its commercial operations while both were extremely wary of the possible impacts from the EU's recently enacted NIS Directive. Another concern from the OES was anything that might affect the monthly payroll run for 17,000 staff worldwide.

Taking these as my high-level requirements, the business need was to focus on the security aspects for the tech refresh of the corporate environment. One of my first tasks was to quantify the risks and propose an appropriate NIS Directive compliant risk management programme. Since the corporate system environment was both large and complex, I was assisted by several of my team and delegated tasks to them whilst maintaining visibility and ownership. For example, I tasked one with analysing and extracting security requirements from relevant legislative requirements e.g. NIS, GDPR, DPA, SOX, OSDR 2015 etc, another with review of all available technical design docs and a third with assimilating existing risk mitigation plans and contractual terms and conditions. Throughout this process I maintained constant communication and buy-in with key stakeholders.

The NIS directive didn't specify a particular Risk Methodology so, together with the stakeholders, we identified and discussed a number of options for quantifying security risk, including IS1 / 2; NIST 800-53; ISO27000; COBIT and OCTAVE. Most were discounted on the basis of cost, unfamiliarity or impracticability before I convinced them that the SANS top 20 CIS security controls could be used as a framework to identify which security measures were in place and effective and which could be improved, all balanced against a comprehensive Threat, Vulnerability and Risk Analysis which would define the major risks to the system.

Commented [A1]: (1.a; 1.b and 1.c) Business Need

Commented [A2]: (2a) Understanding, supporting and enabling Security Governance

Commented [A3]: (2.b) Communicating risk and security concepts effecutively

Commented [A4]: (1.c) Security must support organisational pririties and needs.

Commented [A5]: (1.a) Security requirements support Business Need

Commented [A6]: (3.a) Fundamental principles of Risk Assessment.

Commented [A7]: (3.b) Suitable risk assessment methodologies and awareness of their strengths and weaknesses.

Commented [A8]: (3.f) Understanding system security characteristics and
(3.g) Combining Risk components to assess risk meaningfully.

I also discussed the benefit of taking a top-down view to ensure we incorporated all relevant risks as well as the bottom-up or component driven approach of most common methodologies. Once this was agreed, I led a Business Impact Analysis workshop which identified very sensitive commercial data; R&D intellectual property; significant amounts of personably identifiable information and over $6 Billion a month in financial transactions as the organisations' critical assets on the corporate network. I then directed one of my team to produce a bespoke, detailed threat assessment based on current known industry threat scenarios and internal data of historic security incidents, including a number of attempted insider fraud cases, together with vendor reports and OSINT data going back at least 10 years of attacks on companies of a similar size or in the same industry sector. This identified a complete range of relevant threat actors from Nation States down to script kiddies. Since we had neither the capability or skills internally, we contracted an external provider to investigate our global digital footprint including searching for exposed credentials or other indications we were being actively targeted by any of these Threat Actors.

My team's physical audit produced an unexpected result when we discovered that the OES used a 14 year-old legacy home broadband router to operate a discrete salaries and pensions payments system for foreign staff. This was not in scope for the MSP or me as CSO but, on investigation, was susceptible to a man-in-the-middle attack that could allow an external attacker to divert an entire monthly payroll of tens of millions of dollars. An easy target for at least one nation state actor who had a history of financial cyber-crime. I explained this to the Stakeholders and recommended that the Overseas Salaries system be brought into my scope and the home router immediately replaced with a commercially assured version business class router whilst we redesigned the system and brought it under the Protective Monitoring capability. Not surprisingly, they agreed.

Once the audit was complete, I selected one of my most senior consultants, an experienced ISO 27001 lead auditor supported by a senior Security Architect to conduct the SANS baselining. I gave them two months to complete the task, instructing them to report back at least weekly and if they met any difficulties. All of the collected information was provided to me for analysis, assessment and compilation of the final report. The Risk Assessment phase culminated in a formal briefing by me to the key stakeholders, supported by a number of written reports detailing precisely how and where in the lifecycle each of the 149 SANS 3PT sub-controls had been implemented against the critical assets from the Business Impact Analysis workshop; what remained outstanding; using Attack Trees to graphically show the types of attack that still posed substantial threats and ultimately the level of risks to which the critical business assets were still exposed.

I looked at each of the SANS controls that was either not implemented or not under consideration and assessed how effective it would be at mitigating the threats to the critical assets identified in the BIA and Threat Assessment. At this point, we had the first objective view of the risk picture, allowing the Business to consider spending their limited budget in areas that would have the highest benefit and be future proof against the as yet poorly defined NIS Directive requirements. I also pointed out that mitigating some risks from nation state attackers was well beyond our budget and that these would either need to be accepted or transferred to the Regulator.

My team engaged with current ops, support and the MSP projects teams to ensure that none of the suggested mitigations would adversely impact the business' 24 / 7 / 365 operations or impending technical refresh. Each of the controls was then costed by the MSP and prioritisation agreed between me and the OES stakeholders with some being 'quick wins' and others being longer term aspirations. I was required to manage a constant tension between the MSP's desire to limit costs, maximise their profits and only deliver to the contract and the OES's need to minimise its business risks. Another complexity was the need to secure both the current system and the planned tech refresh / future state. With this in mind, I produced an Implementation Roadmap for all of the proposed controls aligned to and integrated with the Tech Refresh programme roll-out e.g. incorporating application-level monitoring inside the main Oracle Db where all of the commercially sensitive and IP R&D data resided.

The Implementation Roadmap included a comprehensive rolling assurance plan including sourcing hardware and software wherever possible from assured suppliers; post commissioning testing and flowing security

Commented [A9]: (3.d) Combining Top-down and Bbottom up approaches.

Commented [A10]: (3.e) Explanation of Threat Assumtions and sources of information.

Commented [A11]: (4.c) Understanding of some technology areas.

Commented [A12]: (3.c) Impact of risk realisation well understood in business terms.

Commented [A13]: (5.b) Assurance approaches.

Commented [A14]: (4.e) Role of technical, physical, personnel and procedural controls through life

Commented [A15]: (4.a) Traceability between risks, and risk mitigation measures.

Commented [A16]: (4.b) Contextualised security advice.

Commented [A17]: (4.e) Understanding of Risk acceptance / transferral.

Commented [A18]: (4.b) Contextualised security advice.

Commented [A19]: (4.c) Understanding of some technology areas.

requirements to our Supply Chain. I also replaced the previous single system wide annual pen test with a series of component level tests for every phased roll-out during the tech refresh on the grounds that otherwise it could be up to a year after a new application or piece of hardware was introduced before any tests were conducted. I also contracted three different CREST companies to ensure that every test looked for something new rather than basing its actions on previous findings.

The conclusion of the process was a series of formal and informal updates by me to the customer including a high-level overview of the 149 sub controls, their appropriateness to the business and how we would provide them with the confidence that the controls they had approved were cost effective together with the Residual Risks that were beyond their financial envelope for mitigation.

Certified Cyber Professional sample case study 1: satellite services provider

In April 18 I was appointed as the first Global Security Operations Lead for Stardust. Stardust was an ambitious start-up planning to be first global telecommunication company to provide 4/5G and Broadband globally from its own constellation of 800 + small and cheap but high-capacity Low Earth Orbit (LEO) satellites. The technology requires a secure global ground network of 80+ terrestrial locations interconnected with a number of "ground stations" used to control and provide services via the satellite constellation. Stardust and its partners have launched 68 satellites to date using launch sites in Russia, Kazakhstan, French Guiana and the USA.

My review of the board's PESTLE and SWOT analysis showed their level priorities/objectives for security were to continually identify and review the real-world threat picture that evolved with the company's rapid growth and ensure that all business assets were appropriately protected based on business criticality whilst meeting/supporting all mandatory compliances.

I directed a significant effort across the security team to create a documented understanding of the company's current and future business objectives and its essential business processes and assets. This was essential to establish the various relevant threat / attack vectors, identify the vulnerabilities they could exploit and the most cost-effective controls that could be used to mitigate the associated risks sufficiently. My core team of five worked with the wider business and the Governance Risk and Compliance team to produce a formal BIA. We then examined a number of methodologies including CRAMM, IRAM2 and NIST, adapting the best aspects to incorporate both bottom up and top down views in a comprehensive risk assessment.

Additionally, we identified several mandated compliances (US DoD ITAR/EAR and SOX etc) and some aspirational future certifications and associated compliances were discussed (ISO27001/2 etc). I identified that, in the various stages of business development, the threat and risk picture would also evolve from first launch through to full constellation, then establishing a customer engagement portal and the onboarding of customers and delivery of services. Taken together, this gave us a clear, prioritised view of the risks the business faced, the highest being from an attack on launch assets.

My next task was to work collaboratively with other business groups to advise on the security control requirements based on the risks in the current business development and operating model, mandated security compliances and the real-world threats / risks that the future operating model faces supported by recommendations from some early security incident investigations. My first recommendation was to specify, design, build and operate a Security Operations capability based on the MITRE framework to monitor all launch related assets with a service development team in the UK and 24/7 security analyst / ops teams in the US providing effective security risk mitigation delivering prioritised and defined through life security services (technology, process and people) to relevant business areas including:

1. Managed End Point Protection (including anti malware);
2. Vulnerability Management and Patching integrated with service management technologies. (and targeted IT Security Health Checks / Pen Testing);

Commented [A20]: (5.a) Through life assurance.

Commented [A21]: (5.b) Different assurance approaches.

Commented [A22]: (4.d) Rsks cannot always be mitigated.

Commented [A23]: High Level Requirements b. : Within last 7 years.

Commented [A24]: High Level Requirements c. Relevant to the level of risk management specialism for which the candidate is applying and
High Level Requirements d. Role relevant to the level of risk management specialism for which they have applied and .
High Level Requirements f. The level of responsibility claimed in the case study must be appropriate

Commented [A25]: High Level Requirements e. The size, value, complexity and strategic importance of the case study must be appropriate for the level of the application

Commented [A26]: (1.b) Use of different techniques to understand business need.

Commented [A27]: (1.a) Security requirements directed by overall business need.

Commented [A28]: (3.f) Determine and understand the security characteristics of a complicated or novel system in order to understand actual or potential vulnerabilities.

Commented [A29]: (3.a) Expert understanding of the fundamental principles of risk assessment

Commented [A30]: (3.b) Comprehensive risk assessments for complicated or novel scenarios adapting appropriate methodologies where necessary and
(3.c) Top-down and borttom-up views.

Commented [A31]: (3.a) Expert understanding of the fundamental principles of risk assessment

Commented [A32]: (1.c) Articulate how and why these needs support the overall business aim

Commented [A33]: (3.g) Combine to produce meaningful assessment of risk.

Commented [A34]: (4.b) Contextualised security advice appropriate to the overall business need including the sociotechnical considerations of the wider system.

Commented [A35]: (5.b) A range of specific assurance approaches to provide overall confidence

Commented [A36]: (4.b) Contextualised security advice appropriate to the overall business need including the sociotechnical considerations of the wider system.

3. Integrated AI / ML Threat Management (network activity security monitoring);
4. Real time threat Intelligence led operations;
5. Security Incident and Event Monitoring (targeted log sources with associated alerts / reports) including Alarm / CCTV feeds from global satellite earth stations;
6. Data Security Marking and Control (including DLP);
7. Security investigation and Incident management;
8. Global 3rd Party service provider governance monitoring and management.

The first two were specified, designed, installed and began operations as a matter of urgency to protect the infant production infrastructure and applications supporting the first satellite launches together with the HR admin and finance functions. This required a flexible approach as part of the future business model was a full migration from on premises architecture to multiple PaaS; SaaS and FaaS cloud services. I instigated and oversaw the completion of security product / vendor selection via documented RFP/Q processes, blue printing exercises and multi-stage capability assessments involving all stakeholders. This was followed by financial discussion / approval within the senior management team. In each instance, a business case was provided that justified the funding of each security service architecture through life. The deployment of each service followed a plan that I created for the full scope of delivery and associated risk mitigation benefits and the dependencies on other parts of the organisation to assist in deploying agents to assets and enabling communications paths for management functionality. The various risk treatment objectives and appropriate intrinsic/extrinsic/operational/implementation assurance activity were linked back via "use cases" to specific identified and prioritised risks within the business environment. I also made it clear that not all risks, for example a nation state attack on launch capabilities could be effectively mitigated and, as a commercial organisation, Stardust would need to accept those it could not either treat, transfer or terminate.

The company planned to launch more satellites from launch sites in Russia and Kazakhstan ready to deliver services and to prepare for customer access to services via a number of internet facing touch points. This increased security threats / risks significantly in the build up to and over the launch window to the launch operation assets across the globe. There was an increase in risks to the live launch video feeds provided via the company website and directly to other news organisations. The increases in publicity introduced new business threats / risks that needed to be addressed. I also trialled an outsourced real-time external global threat intelligence feed to monitor launch assets for signs of possible attack related intelligence to assist 24/7 monitoring, alerting and response.

The service operation teams adopted ITIL / eTOM principles, and I ensured that the security operations service delivery supported this using documented service models including RACI and Playbooks to identify security responses to identified risks and threats. We also support technical incident remediation using our maturing visibility of network and end-point usage and activity. Current activities include establishing 3rd party governance for existing specialist PAAS/SAAS application providers. Many of the pre-defined contracts did not specify security requirements, and those that existed were scattered throughout contract documentation. These were extracted into a single compliance view and through careful negotiation (avoiding expensive change) I established and maintained a new governance process. In one case this included the provision of a security service portal through which Stardust's SOC team can review security service delivery activity (SIEM / HIDs / NIDs VM etc) and query anomalies directly with the service provider.

I identified a significant area of business risk to senior management concerning data loss/leakage especially DoD ITAR/EAR data as an ITAR breach could have had massive repercussions regarding future use of US tech. With the Board's approval, I commissioned use of Microsoft Azure Information Protection meta data tagging technology based on a documented view of data sensitivity classifications and current data usage to securely manage and monitor the use of sensitive data in business processes. This required SME support from Microsoft to establish their product functionality and has been extended into cloud service environments and supports the deployment of Cloud Access Security Broker and Unified/Data centric security controls.

Commented [A37]: (4.e) Technical, physical, personnel and procedural controls as a through-life activity.

Commented [A38]: (5.a) Through-life assurance at a servie level.

Commented [A39]: (2.a) Enabling decision makers to make well informed decisions.

Commented [A40]: (5.a and 5.b) - Assurance.

Commented [A41]: (4.d) Risks cannot always be fully mitigated.

Commented [A42]: (3.a) Understanding of the fundamental principles of risk assessment.

Commented [A43]: (3.e) Use of various information sources.

Commented [A44]: (2.b) Embedding risk management processes into corporate governance

Commented [A45]: (2.b) Embedding and integrating risk management processes into corporate governance.

Commented [A46]: (2.c) Comunicate difficult risk and security concepts effectively and
(3.d) Impact of risk realisation directly mapped back to business priorities and concerns.

Commented [A47]: (4.c) Competence and understanding across a range of technology areas

Commented [A48]: (4.c) . drawing upon, using and directing appropriate expertise.

This delivery includes a live data security compliance dashboard and material for inclusion in education and training encouraging users to adopt the marking scheme consistently and apply appropriate markings to all documents that they create as pre-cursor to more automated data management.

I recommended and established a permanent live threat intelligence managed service capability (Digital Shadows) focused on the company's business sector threats and specific company and asset to enable the SecOps team to brief business leads inform event planning and propose effective mitigations. This was used to provide threat intelligence to commercial / HR / Operations etc ahead of the satellite launches. This has been tuned to focus on Stardust's assets and activities and the output is shared amongst a number of interested parties. The output is real time and changes as the threat picture evolves to provide a more up-to-date picture of real-world threats than the traditional "snapshot in time" view.

Certified Cyber Professional sample case study 2: HMG cloud migration

In 2019 I was the Lead Consultant for a specialist security service integrator on a circa £7 million contract to guide and facilitate the move of a UK Central Government Department from traditional accredited fixed perimeter security model to a more flexible zero trust model utilising cloud security technologies provided by Azure and AWS. Operating as a UK OFFICIAL environment, the Department has around 320 staff in its London office and business export managers located remotely across the UK and around the world. It sees itself as a global commercial business enabling function with links to HMG and wishes to adopt a more commercial business model and increase representation across many more countries. The business export managers are the customer-facing representatives that aid UK companies and use a variety of SAP based business applications to ensure they have access to the financial support they need. The extant business architecture was largely traditional on-premises networks with bespoke applications hosted in data centres, all delivered to managed endpoints and supported via a single MSP. The move to a zero-trust model was in tandem with a program of change to their business IT environment and support model and driven by the need to operate a more flexible and cloud services focused business model. The existing security model was operated by a small in-house security team and was very HMG compliance focused, lacking the flexibility and agility to support their new business model.

In order to produce a business Impact analysis linked to all known business assets and their vulnerabilities, I began by looking at the broader business context through reviewing the external website and board level planning papers and holding stakeholder workshops.

This was followed by a detailed discovery and prioritisation of current and future business assets; assimilation of existing security risk analysis and risk management / treatment documentation. The existing documentation was largely compliance focused and did not represent any attempt at threat modelling, failed to link assets and vulnerabilities and was not a true reflection of the business risks faced by the Department or an agreed mitigated risks / accepted risk balance. This was also true of the risk treatment plans and limited SecOps capability. I presented these findings to the board and business leads with a high-level action plan to move away from legacy compliance based bottom-up technical risks assessments and rigid application of constraining architectural principles to an ISO-IEC 27001/2 and OCTAVE based top down approach that mapped true business risk and involved business group owners in the 4 phases of implementation and operation.

The approach was accepted by the senior management team and commenced with a series of risk management training sessions and workshops that I organised and supported for the in-house Governance Risk and Compliance team, identified business managers / representatives and the business change program team leads. My threat picture was based on previous security incidents, OSINT research and a classified brief from NCSC. Given that the system was only OFFICIAL, I gained approval to discount threats from nation state actors. Major risks I identified included breaches of data confidentiality that, in addition to attracting fines from the ICO, would also seriously damage the department's reputation, seriously delaying its worldwide expansion plans.

Commented [A49]: (3.e) Use of various information sources.

Commented [A50]: High Level Requirements a. no more than 2 sides of A4.

Commented [A51]: High Level Requirements b.Within last 7 years.

Commented [A52]: High Level Requirements d. role relevant to the level of risk management specialism for which they have applied.
and
High Level Requirements f. The level of responsibility claimed in the case study must be appropriate.

Commented [A53]: High Level Requirements c. Relevant to the level of risk management specialism for which the candidate is applying
and
High Level Requirements e. The size, value, complexity and strategic importance appropriate for the level of the application.

Commented [A54]: (1.a) The ability to elicit complicated, non-obvious security requirements that are directed by the overall business need.

Commented [A55]: (1.b) The use of different techniques to arrive at an understanding of needs in complicated scenarios.

Commented [A56]: (3.a) An expert understanding and evidence of application of the fundamental principles of risk assessment.

Commented [A57]: (3.g) How they 'combine' all of the components of risk in order to arrive at a meaningful assessment and articulation of risk.

Commented [A58]: (3.c) Understanding the need to take both a top-down view of risk as well as more traditional component-based risk assessment activity

Commented [A59]: (1.c) The ability to articulate how and why these needs support the overall business aim of the system/service under consideration.

Commented [A60]: (3.b) The ability to deliver, or enable the delivery of, comprehensive risk assessments for complicated or novel scenarios applying methodologies tha...

Commented [A61]: (2.c) The ability to communicate difficult risk and security concepts effectively in accessible ways that can be clearly understood by business leaders.

Commented [A62]: (2.b) Playing a key role in embedding and integrating risk management processes into appropriate corporate governance processes and business activities.

Commented [A63]: (3.e) Clear explanation of threat assumptions made and the use of various information sources to illuminate their threat assumptions.

Commented [A64]: (3.d) The impact of risk realisation will be well understood and directly mapped back to business priorities and concerns.

After I had completed my analysis, I recommended to the senior management team that to safely adopt a zero trust model in the future, the department would need to improve a number of functions including: user authentication and authorisation to access assets, apply rigorous implementation of the least privilege access principles and careful logical security zoning of the business architecture, supported by asset / risk targeted monitoring, alerting and response.

I recommended several initial security risk treatment strategies to the senior management team, all linked to the highest priority identified risks which in turn were linked to business aims as ratified in workshops with key stakeholders, including:

1. The new approach to business security risk in a zero-trust environment that included the need for through life asset impact assessments. The need for real time cyber assurance evidence using service management tools and cloud security health dashboards (Azure SCC / "Security Score" and AWS Scout suite / prowler dashboards etc).
2. Creation of new security policies, procedures and standards (IDAM / RBAC / Vulnerability and patching standards etc) and their effective dissemination to educate users and support the security technology configurations / processes that will be adopted.
3. Creation of security in design principles and establishment of coordinated devolved responsibility for security within business units. This was given a significant level of urgency due to the need for security support to the impending migration from on traditional on-prem / perimeter protected to cloud hosted business architecture and applications.
4. Risk justified identification and design of effective risk mitigating security protective and detective services (Technology / process / people) that would be supported and operated by an appropriate security analysis and response team using inbuilt cloud security technologies.
5. Migration of JML output to a new IDAM / RBAC model utilising cloud technologies (MS MIM / AWS IAM) linked to application access control and data labelling and management functionality.
6. Establishment of audit based and real time metric 3rd party security governance views e.g. provision of security service integration or delivery evidence clauses in all 3rd party contracts.
7. Robust tested end-point device security policy and managed security technologies including CYOD and cautious BYOD device security and management.

In each case I identified and documented an appropriate strategic approach to recognising and addressing the issues and risks and supported the technical and business development teams allocated to delivering the required functionality and agreed security risk mitigations. Assurance was provided via a detailed set of KPI driven dashboards that gave a real time view of security levels achieved driven by metrics drawn for the various cloud security functions. This was further supported by a series of focused IT Security Health Checks (ITSHC's) and red team exercises provided by a selected security service supplier. The focus for these ITSHCs was primary security controls and areas where previous breaches of security and "near misses" had occurred. The scoping of these test had to consider service provider and contractual requirements in areas where platforms/applications/function and been outsourced through cloud service contracts.

A specialist cloud security architecture development team was engaged to enable and configure the new cloud-based security technologies. Recognising that not all risks can be fully mitigated and using the output from the new business risk focused risk analysis, I identified the various security services that would be needed to adequately mitigate the most serious residual risks and agreed the technologies/vendors and security service scopes with the business stake holders. Budgets and additional licence subscriptions were agreed with cloud service providers and specialist security engineering capability for initial setup was identified. Planning included initial set up and then development of individual SecOps service capabilities including the provision of compliance evidence dashboards and KPI views for management. I drove the capability development by identifying risk focused log feeds and directed the deployment of security monitoring agents on end points, log generation in cloud infrastructure environments and hosted

Commented [A65]: (2.a) The ability to enable decision makers to make well-informed, balanced and cost-effective risk management decisions on situations with complex scope or significant risk.

Commented [A66]: (4.a) Requirement for clear traceability between the most significant identified risks and the measures designed to manage those risks effectively

Commented [A67]: (3.f) The ability to determine and understand the security characteristics of a complicated or novel system in order to understand actual or potential vulnerabilities

Commented [A68]: (4.e) A clear understanding of the various approaches to addressing risk and the role of technical, physical, personnel and procedural controls as a through-life activity.

Commented [A69]: (5.a) Understanding of different approaches through-life assurance at a service as well as a component level.
and
(5.b) The ability to combine a range of specific assurance approaches to provide overall confidence that the things the business values are appropriately protected with clear understanding of the pros and cons of each approach.

Commented [A70]: (4.d) An understanding that risks cannot always be fully mitigated.

applications. Some SaaS applications were onboarded by agreeing and configuring appropriate log feeds supported by service providers/service contracts. Cloud security service technologies selected and in the process of being enabled include:

- SIEM - AWS Guard-duty / Cloudwatch and Azure Sentinel
- IDAM / RBAC - Microsoft Identity Manager (MIM) and PKI certificate services and AWS Identity and Access Management (IdAM)
- Vulnerability Management - AWS Inspector / MS Azure Security Centre
- DSMC / DLP and data labelling - AWS Macie / Azure Information Protection (AIP)
- Global threat intelligence - Digital Shadows

I am currently working with the senior management team to identify a hybrid Security Operations Centre service delivery capability to identify which SOC functions can be outsourced to service providers with appropriate governance / escalations and Key Performance Indicators (KPIs) which should be managed via an in-house security analyst team to assure outsourced service quality. The through life cost of in house SOC services is being carefully balanced with the need to ensure that robust alerting and response to serious incidents is in place. Artificial Intelligence and Machine learning capability is under evaluation to identify what levels of security automation can be used safely to reduce the dependency on manual event analysis and response.

Commented [A71]: business need including the sociotechnical considerations of the wider system. (4.c) Competence and understanding across a range of technology areas

Commented [A72]: (4.c) Using and directing appropriate expertise to solve the bigger security problem.

Commented [A73]: (4.b) The ability to deliver contextualised security advice appropriate to the overall business need including the sociotechnical considerations of the wider system

Commented [A74]: High Level Requirements a. not be more than 2 sides of A4.

Appendix B: Pro forma for the assessment of case studies

This report will be completed by the lead assessor reviewing the case study. A maximum of two case studies can be submitted and this assessment report should be written as a review of all the evidence submitted. Assessors must ensure they discuss case studies with the relevant referee(s), details of whom will have been provided by the applicant. The referees should be able to confirm that the case study accurately describes the work undertaken by the applicant (and not others in the team), and that it is a true record and reflection of the applicant's work.

Requirement	**Confirmed Yes/No**	**Comments**
Does the Case Study describe work carried out within the last 7 years?		
Were the role and level of responsibility of the applicant in this case study relevant to the level of risk management specialism for which they have applied?		
Is the size, value, complexity and strategic importance of the case study appropriate for the level of the application?		
Has the detail of the work completed in the case study been verified by the referee(s)?		
Case study requirement	**Sufficient / insufficient evidence**	**Justification for decision, plus any additional comments or observations**
No.1 – Business need		
No.2 – Security direction and governance		
No.3 – Risk assessment		
No.4 – Risk treatment		
No.5 - Assurance		

Is there enough evidence in the case study to provide a sound basis for an interview? ☐ Yes ☐ No

Appendix C: Specialist interview pro forma (consultancy skills for both Associate Cyber Professional and Certified Cyber Professional)

Consulting skills and behaviours The following consulting skills are a set of behaviours that cyber security professionals will need to exhibit to be effective in their roles as advisors to clients. They are comprised of 3 elements: interviewing and empathy, appropriate style and clear delivery and facilitation.			
Skill	**Fail – bad indicators**	**Pass – Good indicators**	**Comments**
Interviewing and empathy	• Unable to understand or relate to the business needs of a client. • Needs active supervision to ensure the client's business priorities, technical context and timescales are fully explored.	• Engages effectively with the client to understand needs and drivers. • Understands the business context and the agenda of the stakeholders. • Balance of talking and listening (70 – 30). • Concerned and inquisitive.	
Clear delivery and appropriate style	• Does not organise arguments well and tends to mix key issues with trivia. • Finds it difficult to adapt style to different levels of audience. • Tendency to ramble and describe too much detail. • May interrupt the speaker.	• Presents arguments in a clear and articulate manner selecting the appropriate level of detail to suit the audience. • Good eye contact. • Effective time management.	
Facilitation	• Unable to take an independent position. • Unable to ensure that all voices are heard. • Likely to find it difficult to manage conflicts.	• Is able to build consensus, manage conflict and achieve conciliation, and offer arbitration. • Keen to come to an acceptable conclusion. • Keen to ensure that all parties understand the other party's point of view.	
Summary of overall indicators	• Arrogance • Pomposity • Grandiose • Lack of interest	• Natural/comfortable in demeanour • Confident • Respectful	

Appendix D: Specialist knowledge interview pro forma (Associate Cyber Professional)

1. Establish the business need – 10 to 15 minutes				
Pass indicators	**Fail indicators**	**Sample questions**	**Pass/Fail**	**Comments**
1.Evidence of how business needs are gathered and understood, including an understanding of high-level business objectives. 2. Can clearly demonstrate elicitation of straightforward security needs. 3. Understands and can articulate how security requirements directly support the needs of the business. 4. Demonstrates an ability to help an organisation understand their security needs as necessary to support their business objectives. 5. Demonstrates an understanding and ability to balance business objectives and security needs. 6. Can explain how they identify key stakeholders (or their representatives) from within the business and understand their priorities and concerns.	1. Focusses on simple C, I and A (Confidentiality, Integrity and Availability) requirements without business context. 2. Determines business need from just a regulatory or compliance basis. 3.Security does not support and is not mapped to business need or objective. 4. Lack of evidence that the business was appropriately consulted or considered. 5.Unable to demonstrate the ability to map or explain security requirements in business terms.	[explore the process of establishing security requirements based upon business need in the provided case study] Describe a situation where you helped a customer understand and articulate their security needs. 1. How did you approach this? 2.What did you do? 3.What was the outcome? Describe a situation where there was an actual or perceived conflict between security requirements and business need 1.How was the conflict identified? 2.What was your approach to resolving the conflict? 3.What was the outcome?		

2. Security direction and governance (10 to 15 minutes)				
Pass indicators	**Fail indicators**	**Sample questions**	**Pass/Fail**	**Comments**
1.Clearly understands and has evidence of participating within organisational governance mechanisms. 2.Can identify who the real decision makers are with responsibility for the service or system within the scope of the analysis and understands how security impacts upon their responsibilities. 3.A demonstrated ability to articulate security concepts to business leaders or their representatives which helps them to make well informed decisions. 4.Can understand and interpret decision makers' risk appetite statements and tolerances with regards to things that are important. There is some evidence of being able to turn that top-level intent into meaningful security direction. 5.Aware of applicable legislation, regulation and/or standards and the implications in the context under consideration.	1.Does not understand governance structures and decision making in the organisations within the scope of the assessment. 2.Cannot explain risk appetite in a meaningful way or explain how it could be interpreted in the context of the case study. 3.Unable to demonstrate how they work with business direction such as risk appetite and tolerance statements in a meaningful manner. For example, talking about risk appetite in an entirely abstract sense (averse – hungry). 4.A lack of understanding about applicable legislation, regulation and/or standards.	Tell me how governance was approached when you worked with [case study] 1.What was your role and how did you support the governance arrangements? 2.How did you work within these arrangements? How was risk appetite articulated? 3.How did this shape/direct subsequent risk management activities? How were security decisions made? 4.What was your role in supporting or informing those decisions? Were there any legal, regulatory or policy considerations that influenced how security governance and decision making worked? Can you give me an example of where you believed the wrong security decision was made? 5.Why did you believe this was the case? 6.What did you do?		

3. Risk assessment (40 to 45 minutes)				
Pass indicators	**Fail indicators**	**Sample questions**	**Pass/Fail**	**Comments**
1.Can describe application of the fundamental principles of risk assessment to situations of reasonably complex scope. 2.Recognises the need for, benefits and limitations of different types of risk assessment approaches. They can explain a rationale for methods they have used including how they may have modified the method to best suit their context. 3.Can clearly explain how they determine applicable business assets/things of value and the impact to these assets should they be affected or compromised. They undertake this in conjunction with key stakeholders. 4.Clearly explains how they determine an applicable threat model, the vulnerabilities that could be exploited and how this could impact the identified assets. 5.Recognises the limitations of their risk analysis, for example determination of threat motivation or reputational impact. 6.Understands the applicability, benefits and limitations of qualitative versus quantitative analysis methods. 7.Risk assessment output is well constructed, meaningful and tailored to the audience needs. Risks are well contextualised to aid decision making. 8.Able to explain and justify the approach to prioritisation of risks by comparing and balancing different types of risk from across the organisation.	1.The risk assessment approach is process-driven ('turn handle') and shows little flexibility or customisation. There is a lack of understanding of how methods or approaches support fundamental risk assessment principles. 2.The assessment approach is immature and there is a poor understanding of the relationship between the constituent parts of the assessment. 3.The approach to analysis is inflexible with a preference for applying one approach to all aspects of risk assessment. 4.Refers to impact assessment in an abstract sense, such as simply by reference to classification. 5.The understanding of threat is immature, and sources of threat information are used without understanding or contextualization. 6.Risk assessments are conducted in isolation of the business objective. 7.Qualitative and quantitative approaches are confused and not used appropriately. 8.A process only based approach to presentation and prioritisation is followed, for example by combining abstract criteria using a matrix. 9.Risks are prioritised and presented in the same way irrespective of the audience. 10.Risks are presented and prioritised in a biased way so that the audience is drawn to improbable or unrealistic risks.	Talk through the approach to risk assessment when you worked with [case study] 1.Did you work with a specific risk assessment method? 2.Why did you choose to work with that method? 3.What modifications did you need to make for your situation? How did you identify the scope of the assessment and how did this determine the approach taken? Can you explain your approach to identifying key assets? 4.What was identified and why? 5.What did the business care about and why? How did you determine the applicability of relevant sources of threat? 6.How did you validate your threat model? 7.What technical assumptions did you make about the identified threat? How did you assess vulnerability in the system		

3. Risk assessment (40 to 45 minutes)				
Pass indicators	**Fail indicators**	**Sample questions**	**Pass/Fail**	**Comments**
	11.Risks are dismissed and/or prioritised only according to the views of the applicant – there is little indication that the business has been consulted.	or service under consideration? 8.What approaches did you use to support your analysis? How did you gain confidence in your analysis? Talk us through the approach to evaluating, presenting and prioritising the risks you identified for [case study] 9.Can you describe the rationale behind the risks that you had identified and the corresponding severity? 10.Of the risks identified, how did you determine which ones should be prioritised? 11.How do you differentiate between high impact/low probability and low impact/high probability? Other than security stakeholders, were there any other parts of the business that you shared your findings with? 12.How did you ensure they understood the risk presentation? How was the risk assessment received by the business?		

3. Risk assessment (40 to 45 minutes)				
Pass indicators	**Fail indicators**	**Sample questions**	**Pass/Fail**	**Comments**
		13.Were there any challenges to what you presented? In the context of existing answers above what were the top 3 risks identified?		

4. Risk treatment (25 to 30 minutes)				
Pass indicators	**Fail indicators**	**Sample questions**	**Pass/Fail**	**Comments**
1.Able to articulate evidence of developing risk mitigation strategies that manage specific and defined high magnitude risks. 2.Can describe the creation of risk mitigation strategies to mitigate classes of risks (such as risks arising from 'commodity' internet-based attacks). 3.Demonstrates an ability to understand when and how to use control frameworks appropriately and the classes of risks that can be managed by such. 4.Mindful of different risk treatment options (treat, transfer, accept etc) and uses organisational direction to influence recommended treatment options. 5.Recognises the limitations of risk mitigation approaches and the need to manage residual risk appropriately. 6.Understands and can demonstrate the need for holistic mitigation based on physical, personnel, procedural and technical control types. 7.Understands that systems change (for example, operational need changes, threat changes or emergent vulnerabilities), so management needs to be ongoing. 8.Understands when security measures might impact on users or business needs and is able to provide effective advice to help the business make appropriate decisions. 9.Delivers security advice that is contextualised and	1.Risk treatment is described in isolation from the business, without empowering the business decision maker regarding treatment options. 2.Unclear how recommended controls actually mitigate the identified risks whilst supporting the business need. 3.Risk mitigation tends to be dominated by the use of standard control frameworks and they're unclear when that may not be appropriate. 4.The approach to risk treatment is based solely upon compliance, rather than management of actual risk. 5.Does not recognise when security measures might impact users or business needs. 6.Unable to provide security advice in a contextual manner appropriate to the circumstances in which they are working. 7.Risk treatment is considered only at a single point of time (such as an accreditation milestone) rather than throughout the whole lifecycle.	Talk through the approach to managing the top 3 identified risks for [case study] 1.How did you decide and agree upon the suitability of the controls? 2.How did you ensure that the approach will remain effective throughout the system lifecycle? How did you ensure traceability between the assessed risks and the subsequent mitigation activities? Did you work with any control sets to support treatment? 3.If so, how did you work with them? 4.What were the pros and cons of those control sets? Can you give me an example of where you were asked to justify a specific mitigation to the business? Were there any situations where it was not possible to mitigate a risk? 5.If so, what did you do?		

4. Risk treatment (25 to 30 minutes)				
Pass indicators	**Fail indicators**	**Sample questions**	**Pass/Fail**	**Comments**
appropriate for the customer need. Avoids providing 'point' solutions or advice that does not address the overall key security issues		How were residual risks identified and how were these managed? Can you describe a situation where you were required to explain a complex security recommendation to a senior person who did not have the time or technical knowledge to understand the problem? • What approach did you take? • Was the person able to make an informed judgement? Describe a situation when you have provided advice to defend against a potential future risk rather than a visible current one. Sample technical questions may also be asked, examples of which can be found at Appendix I.		

5. The assurance approach (15 – 20 minutes)				
Pass indicators	**Fail indicators**	**Sample questions**	**Pass/Fail**	**Comments**
1.Understands different sources and approaches for gaining assurance. This includes a clear understanding of the benefits and limitations of different assurance techniques. 2.Applies a range of assurance approaches to solutions, with a clear understanding of the strengths and limitations of each approach.	1.There is little awareness of the need for assurance. 2.The approach to assurance is driven solely by compliance with artefacts such as classification. 3.There is evidence of a dogmatic approach to assurance for example mandating certified products without clear reasoning.	Talk through the approach to assurance for [case study] Can you provide some examples of assurance activities and explain the pros and cons of them? How did you demonstrate confidence to a business leader or their		

3.Assurance and confidence are not limited to a point in time, but the applicant seeks to address confidence across the system/service lifecycle. 4.Understands and applies different approaches to product, implementation and operational assurance. Uses each appropriately to derive a genuine understanding of confidence that the overall business objective is protected.	4.The applicant focuses on specific aspects of assurance activity rather than determining overall confidence at a system level. 5.Assurance is conducted at a single point in time rather than across the lifecycle of the system/service. 6.Cannot explain how different approaches to products, implementation and operational assurance can be effective.	representative that their overall concerns were appropriately protected? Can you give an example of where you have had to provide confidence that risks will remain managed through system life?		

Appendix E: Specialist knowledge interview pro forma (Certified Cyber Professional)

1. Establish the business need (10 to 15 minutes)				
Pass indicators	**Fail indicators**	**Sample questions**	**Pass/Fail**	**Comments**
1.Evidence of how business needs are systematically determined, gathered and understood, including an understanding of high-level mission objectives. 2.Understands and uses appropriate methods and techniques for establishing business need. 3.Can demonstrate elicitation of complicated, non-obvious security needs. For example, where the mapping between business need, the technology that supports that need and how it might be impacted is non-trivial to deduce. 4.Understands and can articulate how security requirements directly support the needs of the business. 5.Demonstrates an ability to help an organisation reason about their security needs as necessary to support their business objectives. 6.Demonstrates an understanding and ability to balance what may appear to be competing needs	1.Focusses on simple C, I and A (Confidentiality, Integrity and Availability) requirements without business context. 2.Determines business need from just a regulatory or compliance basis. 3.Security does not support and is not clearly mapped to business need or objective. 4.Lack of evidence that the business was effectively consulted or considered. 5.Did not provide evidence of adapting the service offering in response to business needs. 6. Shows a lack of understanding of standardised ways of determining security requirements. 7.Unable to demonstrate the ability to map or explain complicated security requirements.	[explore the process of establishing security requirements based upon business need in the provided case study] Describe a situation where the customer was unable to clearly articulate their security requirements 1.How did you approach this? 2.What did you do? 3.What was the outcome? Describe a situation where there was an actual or perceived conflict between security requirements and business need 1.How was the conflict identified?		

1. Establish the business need (10 to 15 minutes)				
Pass indicators	**Fail indicators**	**Sample questions**	**Pass/Fail**	**Comments**
between business objectives and security. 7.Can explain how they identify key stakeholders from within the business and determination of their priorities and concerns.		2.What was your approach to resolving the conflict? 3.What was the outcome? Describe a situation where the customer didn't agree with your assessment of security need. 1.What was the basis of the disagreement? 2.How did you respond? 3.Were you able to come to an agreement?		

2. Security direction and governance (10 to 15 minutes)				
Pass indicators	**Fail indicators**	**Sample questions**	**Pass/Fail**	**Comments**
1.Clearly understands and has evidence of shaping organisational governance mechanisms. This may include establishing new, effective governance mechanisms or demonstrating expert use of more complex existing processes to support a given project or system. 2.Can identify who the real decision makers are with responsibility for the service or system within the scope of the analysis and help them understand how security impacts upon their responsibilities. 3.A demonstrated ability to articulate complex security concepts to business leaders and decision makers which enables them to make well informed decisions. 4.Helps decision makers deduce their risk appetite and tolerances with regard to things that are important to them. There is evidence of being able to turn top-level intent into meaningful direction for others. 5.Aware of applicable legislation, regulation and/or standards and the implications in the context under consideration.	1.Does not clearly understand governance structures and decision making in complex organisations or situations. 2.Can only demonstrate an ability to work within established and well-defined existing governance structures. 3.Cannot explain risk appetite in a meaningful way or explain how it could be interpreted in the context of the case study. 4.Unable to demonstrate how they work with decision makers to understand and deduce risk appetite and tolerances in a meaningful manner. For example, talking about risk appetite in an abstract sense (averse – hungry). 5.A lack of understanding about applicable legislation, regulation and/or standards	Tell me how governance was approached when you worked with [case study] 1.What was your role in establishing governance arrangements? 2.How did you work within these arrangements? How was risk appetite determined and articulated? 3.How did this shape/direct subsequent risk management activities? How were security decisions made? 4.What was your role in supporting or informing those decisions? Were there any legal, regulatory or policy considerations that influenced how security governance and decision making worked? Can you give me an example of where you believed the wrong security decision was made? 5.Why did you believe this was the case? 6.What did you do?		

3. Risk assessment (40 to 45 minutes)				
Pass indicators	**Fail indicators**	**Sample questions**	**Pass/Fail**	**Comments**
1.Can describe application of the fundamental principles of risk assessment to situations of significantly complex scope. 2.Recognises the need for, benefits and limitations of different types of risk assessment approaches. They can explain a rationale for methods they have used including how they may have modified the method to best suit their context. 3.Can clearly explain how they determine applicable business assets/things of value and the impact to these assets should they be affected or compromised. They undertake this in conjunction with key stakeholders. 4.Clearly explains in detail how they determine an applicable threat model, the vulnerabilities that could be exploited and how this could impact the identified assets. 5.Recognises the limitations of risk analysis, for example determination of threat motivation, reputational impact or complex system dynamics. 6.Understands the applicability, benefits and limitations of qualitative versus quantitative analysis. 7.Risk assessment output is well constructed, meaningful and tailored to the audience needs. Risks are well contextualised to aid decision making. 8.Able to explain and justify the approach to prioritisation of risks by comparing and balancing different types of risk from across the organisation.	1.The risk assessment approach is process-driven ('turn handle') and shows little flexibility or customisation. There is a lack of understanding of how methods or approaches support fundamental risk assessment principles. 2.The assessment approach is immature and there is a poor understanding of the relationship between the constituent parts of the assessment. 3.The approach to analysis is inflexible with a preference for applying one approach to all aspects of risk assessment. 4.Refers to impact assessment in an abstract sense, such as simply by reference to classification. 5.The understanding of threat is immature, and sources of threat information are used without deep understanding and contextualization. 6.Risk assessments are conducted in isolation of the business objective. 7.Qualitative and quantitative approaches are confused and not used appropriately. 8.Only process based approach to presentation and prioritisation are followed, for example by combining abstract criteria using a matrix. 9.Risks are prioritised and presented in the same way irrespective of the audience. 10.Risks are presented and prioritised in a biased way so that the audience is drawn to improbable or unrealistic risks 11.Risks are dismissed and/or prioritised only according to the views of the applicant.	Talk through the approach to risk assessment when you worked with [case study] 1.Did you work with a specific risk assessment method? 2.Why did you choose to work with that method? 3.What modifications did you need to make for your situation? How did you identify the scope of the assessment and how did this determine the approach taken? Can you explain your approach to identifying key assets, what these were and why? 4.What did the business care about and why? How did you determine the applicability of relevant sources of threat? 5.How did you validate your threat model? 6.What technical assumptions did you make about the identified threat? How did you assess vulnerability in the system or service under consideration?		

3. Risk assessment (40 to 45 minutes)				
Pass indicators	**Fail indicators**	**Sample questions**	**Pass/Fail**	**Comments**
		7.What approaches did you use to support your analysis? How did you gain confidence in aspects of your analysis? Talk us through the approach to evaluating, presenting and prioritising the risks you identified for [case study] 8.Can you describe the rationale behind the risks that you had identified and the corresponding severity? 9.Of the risks identified, how did you determine which ones should be prioritised? 10.How do you differentiate between high impact/low probability and low impact/high probability? How was the risk assessment received by the business? 11.Were there any challenges to what you presented? In the context of existing answers above what were the top 3 risks identified?		

4. Risk treatment (25 to 30 minutes)				
Pass indicators	**Fail indicators**	**Sample questions**	**Pass/Fail**	**Comments**
1.Able to articulate evidence of developing risk mitigation strategies that manage specific and defined high magnitude risks. 2.Can describe the creation of risk mitigation strategies to mitigate classes of risks (such as risks arising from 'commodity' internet-based attacks). 3.Demonstrates an ability to understand when and how to use control frameworks appropriately and the classes of risks that can be managed by such. 4.Mindful of different risk treatment options (treat, transfer, accept etc) and uses organisational direction to influence recommended treatment options. 5.Recognises the limitations of risk mitigation approaches and the need to manage residual risk appropriately. 6.Understands and can demonstrate the need for holistic mitigation based on physical, personnel, procedural and technical control types. 7.Understands that systems change (for example, operational need changes, threat changes or emergent vulnerabilities), so management needs to be ongoing. 8.Understands when security measures might impact on users or business need and is able to provide effective advice to help the business make appropriate decisions. 9.Delivers security advice that is contextualised and appropriate for the overall need. The applicant avoids providing 'point' solutions or	1. Risk treatment is described in isolation from the business, without empowering the business decision maker regarding treatment options. 2.Unclear how recommended controls would actually mitigate the identified risks so as to support business needs. 3. Only able to explain the use of standard control frameworks and unclear when that may not be appropriate. 4.The approach to risk treatment is based solely upon compliance, rather than management of actual risk. 5.Does not recognise when security measures might impact users or business needs. 6.Unable to provide security advice in a contextual manner appropriate to the circumstances in which they are working. 7.Security advice is limited and does not go beyond standard approaches. 8.Risk treatment is considered only at a single point of time (such as an accreditation milestone) rather than throughout the whole lifecycle.	Talk through the approach to managing the top 3 identified risks for [case study] 1.How did you decide and agree upon the suitability of the controls? 2. How did you ensure that the approach will remain effective throughout the system lifecycle? How did you ensure traceability between the assessed risks and the subsequent mitigation activities? Did you work with any control sets to support treatment? 3.If so, how did you work with them? Can you give me an example of where you were asked to justify a specific mitigation to the business? Were there any situations where it was not possible to mitigate a risk? 4.If so, what did you do? How were residual risks identified and how were these managed?		

4. Risk treatment (25 to 30 minutes)				
Pass indicators	**Fail indicators**	**Sample questions**	**Pass/Fail**	**Comments**
advice that does not address the overall key business security needs. 10.Looks at the wider 'system' which includes sociotechnical considerations (e.g., the role the user plays in meeting the desired security outcomes). 11.Security advice offered by the applicant extends beyond particular technologies with which the applicant is familiar and draws upon and directs appropriate expertise. 12.Security advice is appropriate for the development model the customer is following. This might include things such as security in a complicated supply chain through to security in CI/CD environments.		Can you describe a situation where you were required to explain a complex security recommendation to a senior person who did not have the time or technical knowledge to understand the problem. • What approach did you take? • Was the person able to make an informed judgement? Have you dealt with a customer who had a preconceived idea of what the solution should be and you have had to influence their perception? • How did you approach this? • How did you go about getting them to be open to other ideas? • Did they change their position? Describe a situation when you have provided advice to defend against a potential future risk rather than a visible current one Sample technical questions may also be asked, examples of which can be found at Appendix I.		

5. The assurance approach (15 – 20 minutes)				
Pass indicators	**Fail indicators**	**Sample questions**	**Pass/Fail**	**Comments**
1. Understands different sources and approaches to gaining assurance. This includes a clear understanding of the benefits and limitations of different assurance techniques. 2.Applies a range of assurance approaches to solutions, with a clear understanding of the strengths and limitations of each approach. There is a clear ability to map the assurance options recommended directly to the security need to be addressed. 3.Assurance and confidence are not limited to a point in time but the applicant seeks to address confidence across the system/service lifecycle. 4.The applicant understands and applies different approaches to product, implementation and operational assurance. Uses each appropriately to derive a genuine understanding of confidence that the overall business objective is protected.	1.There is little awareness of the need for the assurance. 2.The approach to assurance is driven solely by compliance or artefacts such as classification. 3.There is evidence of a dogmatic approach to assurance for example mandating certified products without context. 4.The applicant focuses on specific aspects of assurance activity rather than determining overall confidence at a system level. 5.Assurance is conducted at a single point in time rather than across the lifecycle of the system/service. 6.Cannot explain how different approaches to products, implementation and operational assurance can be effective.	Talk through the approach to assurance for [case study]. How did you demonstrate confidence to a business leader that their overall concerns were appropriately protected? Can you give an example of where you have had to provide confidence that risks will remain managed through system life? Can you provide some examples of assurance activities and explain what the value of these were? How did you work with the risk appetite to gauge appropriate assurance?		

Appendix F: Application form and declaration for candidates

The following form should be completed on application for a CCP Specialism

Personal Details					
*Name:					
*Email address:					
*Mobile phone number: *Work phone number (if different):					
*Address and postcode:					
*Proof of Foundational Knowledge (see below):					
*Specialism recognition being applied for:					
Case Study (see below)					
Case Study no.	*Name of referee	*Email address of referee	*Contact number(s) for referee	*Referee's organisation and role	*Referee's relationship to applicant
Case Study 1					
Case Study 2					
*denotes mandatory information. NOTE: Referees' permission to be named must be obtained before being provided. All necessary permissions relating to the nature and contents of the case study/ies must be obtained before being provided.					

Foundational Knowledge Requirements

Applicants need to demonstrate proof of foundational knowledge of cyber security by holding one of the following (delete as appropriate):

- An NCSC-certified degree (undergraduate or postgraduate) or
- Certified Information Systems Security Professional (CISSP), including full membership of (ISC)² or
- Certified Information Security Manager (CISM), including full membership of ISACA or
- Full Membership (MCIIS) of the Chartered Institute of Information Security (CIISec) or
- Proof of having passed an appropriate NCSC internal skills level assessment or
- Proof of having completed an internal NCSC professional development framework (for example for cyber security architecture).

Case Study referees

All case studies must be supported by a referee. The same referee may support two case studies if they can genuinely validate both. All referees will be contacted. Applicants must have permission from referees (and other relevant parties, if any) both for the content of the case studies and for supplying their contact details.

Supporting Documentation

The following documents should be provided electronically together with the application form. If you wish to send any of them by post instead, please discuss and agree this in advance with the Certification Body:

- a scanned copy of an officially issued photographic identification
- certificate(s) or other appropriate proof in support of the foundational knowledge requirements above
- a case study (up to two per specialism will be accepted), which describes how you have met all the criteria for the specialism (see pp 7 - 11 of this document)

Special Requirements

Do you have any special requirements for the assessment, for example a reasonable adjustment?

Yes ☐ No ☐

If you answered yes to the above, we will contact you shortly to discuss your requirements. Please note that you will need to show evidence to qualify for any special requirements.

The information supplied will not be used for any purpose other than assessment for the CCP specialism. Interviews may be recorded for the purposes of quality checking and for review in case of an appeal against an assessment decision. Certification Bodies reserve the right to share such data with NCSC for the purposes of oversight of the Certified Cyber Professional assured service. A transcript will be kept for legitimate interest in compliance with the UK GDPR[10] and will be destroyed within 6 months of the interview in line with Certification Bodies' appeals policies**.** Certification Bodies are solely responsible for ensuring they comply with all data protection and data storage requirements

[10] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

Declaration

I confirm that I have read and understood all the above information and will abide by the Code of Conduct at Appendix H.

Name:

Signature:

Date:

Appendix G: Template for CPD/CPE log

Name	Nature of Activity	What did I learn?	What was the outcome?	Name of referee	(to be completed by assessor) Is there sufficient evidence of CPD/CPE?		Assessor's Comments
					Y	N	
Date							
Date							
Date							
Date							
Date							
Date							

Appendix H: Code of conduct

NCSC expects all Specialists undertaking work on the basis of recognition by the NCSC to comply with the following code of conduct.

Attribute	Expected Behaviour	Inappropriate Behaviour
Impartiality	• Acting in the best interests of the client or client organisation at all times.	• Proposing or undertaking unnecessary or excessive work. • Suppressing findings that the client representative does not wish to hear. • Recommending inappropriate products or services. • Not declaring potential conflicts of interest.
Objectivity	• Basing advice on material knowledge, facts, professional experience and evidence.	• Being influenced by personal relationships or short term objectives. • Ignoring material facts and data.
Confidentiality & Integrity	• Protecting information received in the course of work for a client organisation.	• Disclosing vulnerabilities in client information systems to third parties. • Sharing any client information with third parties without permission.
Compliance	• Ensuring that advice and conduct are consistent with applicable laws and regulations.	• Recommending actions that knowingly contravene applicable laws, regulations or policies. • Recommending actions which conflict with NCSC guidance. • Undertaking security testing without client permission.
Competence	• Maintaining and updating knowledge and skills and providing evidence of this. • Ensuring advice is proportionate with business objectives and the level of information risk .	• Undertaking work which you know you are not competent to undertake. • Presenting yourself as having a higher level of competence than is actually the case. • Recommending work that is disproportionately large to business requirements. • Recommending solutions that are grossly inadequate to meet the intended business requirements.
Reputation	• Preserving the reputation of the specialism recognition.	• Conduct that may bring the Certified Cyber Professional assured service into disrepute. • Misrepresenting the specialism and its scope.

Appendix I: Sample technical questions

1. What risk does the padlock in the browser address bar indicate is being mitigated?

A: The padlock in the browser indicates that a client's browser has connected to a webpage 'securely' using HTTPS on port 443.

2. What does HTTPS mitigate?

A: The 'S' in HTTPS stands for 'Secure' – Hyper Text Transfer Protocol Secure – it is an extension of the HTTP protocol. Specifically, HTTPS mitigates the risks posed to the confidentiality and integrity of the data that is exchanged between the client's browser and the web server so that it cannot be read through eavesdropping or Man-in-the-Middle (MITM), attacks or altered by a third-party. HTTPS can also provide authentication for both clients and servers through certificates.

3. What risk does a firewall mitigate?

A: Firewalls mitigate the risk associated with uncontrolled access to a network or network services, typically by tracking the state of connections - only packets matching known permitted connections are allowed to pass through it. Firewalls are typically used between dissimilar security domains such as the Internet and an organisation's private network. Firewalls typically restrict access based on source IP address(es) and TCP socket numbers using rules which form part of the firewall policy. For example, a firewall rule may be established which permits a registered public IP address of a partner organisation on the untrusted network (the interface to the Internet), to access a hosted web service on port 443 on the trusted network, (a DMZ). All other IP addresses would be blocked from accessing that web service, and the partner organisation would only be able to connect to the web service on port 443; as all other TCP socket numbers would be blocked. Firewalls can be network-based or host-based. As well as controlling access to a network or network services, application firewalls can also control input, output and/or access from, to or by an application or service. It does this by inspecting the content of the traffic. Application firewalls are sometimes referred to as a proxy-based or reverse-proxy firewall.