National Cyber Security Centre
a part of GCHQ

# NCSC Certified Cyber Professional (CCP) Assured Service

## Assessment Criteria for Security Architecture Specialism Recognition

=

*Document History*

| Version | Date | Notes |
|---|---|---|
| 1 | January 2022 | Security Architecture 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.

---

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/

6. **Associate Cyber Professionals** can apply their expertise in a range of typical security architecture circumstances, relating it to the fundamental principles of security architecture, for example as an effective and skilled member of a team or within established organisational processes.
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. Application forms may be submitted at any time via the websites of one of the three Certification Bodies (see Appendix F *for an example* of the application form.) along with a short CV of no more than 2 sides of A4 (Arial font size 10) covering their last 5 years of employment and including referees. The referee(s) must be able to vouch for the whole of the period under consideration.
9. The CV should include details of the technical and risk management work undertaken in each role, it should not be a generic CV.
10. Individuals will apply to their certification body of choice. Information about each Certification Body can be found on its website.
11. 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.
12. Approximately 1 hour of the interview will be spent discussing a hypothetical workplace scenario which candidates will receive at least 24hrs in advance of the interview *(see paragraphs 34 & 35 for further details)*
13. 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

14. The aim of the NCSC with regard to foundational knowledge is to ensure that applicants have an approximately commensurate and broad level of cyber security knowledge. This can be demonstrated through academic qualifications, professional certifications, professional memberships, 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) [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); or

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

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

- NCSC Certified Cyber Security Scheme head consultants and NCSC staff members holding a minimum of security architecture skill 6.4 level 3 may vouch for the foundational knowledge of applicants with whom they have worked in the previous 2 years for a period of no less than 12 months.

15. 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. Candidates using the 'vouching' option for foundational knowledge should provide the name and contact details of the person who has agreed in advance of the application to vouch for their foundational knowledge and also provide a short summary of the nature and extent of their working relationship, which must have been for a minimum of 12 months, and recent ie. commenced within the last 2 years. These details should be forwarded to enquiries@ncsc.gov.uk on submission of the application.

## Demonstration of specialist knowledge

16. 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 for verification purposes. The assessment criteria for case studies follow below (see paragraphs).
17. If the case study is accepted, applicants will be invited to attend an interview with Certification Body assessors.
18. 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. The interview assessment criteria follow below (including the final table).

## Fees

19. 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

20. 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.
21. Candidates should not refer to specific customer system names in case studies, as it may limit what can be said at interview regarding risks.
22. 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 in borderline cases, resubmissions which still lack some requisite detail may, at

the assessors' discretion, be allowed to progress to interview in order to determine whether the applicant has the required degree of specialist knowledge application.

## High level requirements

23. 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 diagrams and/or tables to support the main document.
24. The case study must cover work carried out within the last 3 years.
25. 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 the specialism for which the candidate is applying.
26. Details of the work completed in the case study should be verifiable.
27. All case studies should demonstrate:

- The candidate's technical abilities through the specialism. This should include but not be limited to, specific examples of risks and how they were remediated by the candidate in order to demonstrate the level of complexity at which they are working
- 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.

28. 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

29. It is expected that Associate Cyber Professionals can demonstrate a high level of ability in reasonably complex or demanding environments. They will be able to demonstrate good practice and will have delivered excellent results for their clients in all respects. Whilst they may not have the highest level of expertise or experience in all aspects of the security architecture specialism, they will be very clear on their own areas of weakness and should be able to recommend good potential sources of such expertise to assist their clients when required. Their areas of weaker knowledge and/or experience should be limited and should not impact significantly on the main principles of the security architecture specialism. In the requirements sections below, it is expected that those applying at Associate level will be able to demonstrate experience and expertise in the more usual and straight-forward environments where standard solutions and patterns are entirely appropriate. They should be able to demonstrate that they have had to address standard or straight-forward requirements from the business, from the design of the system or from any other source. They will have worked essentially as part of a team or under close supervision within a standardised environment of security architecture and related processes and solutions.
30. The candidate's case study should demonstrate:
    - Clear awareness of the need to provide traceability between business need and security requirements.
    - The ability to review architectures and identify likely attacks for simple or obvious security requirements for highly standardised use cases, using well established guidance. (This is unlikely to be contentious.)
    - The ability to provide security architecture designs to address standard security needs. Advice could be written or verbal.

- An awareness of limitations and scope for what advice can be given and when to draw on others' expertise.
- The ability to meaningfully describe straight-forward security concepts and their business applicability.
- The ability to contextualise security recommendations and risk statements to the business need under consideration.
- The ability to support security professionals in designing secure systems and developing mitigation strategies for relatively common and well understood scenarios.
- An understanding of the fundamentals of risk and risk management processes and decision making.

This can be met through:

- The application of risk assessment and risk management techniques to system designs in order to mitigate security risks; and
- The ability to review security architecture designs to ensure they mitigate identified security risks, whilst balancing an organisation's business requirements, e.g. reviewing systems to ensure that cyber-attacks are mitigated to a reasonable level, (set by the system owner) whilst balancing other factors such as user needs, costs, performance, etc.

## Certified Cyber Professional: additional specific case study criteria

31. A CCP recognised security architect is considered a "leading light" in the architecture community who can review or design the security of any system without supervision in areas with which they are not familiar. They should be able to design the security of new and complex systems using a range of technology, based on a deep technical background and in-depth knowledge and experience of risk management. It is expected that a CCP-recognised architect will be able to work without supervision (although following a robust quality control process) in the design of organisationally important systems which have a complex set of security risks using new forms of technology. Whilst doing this, they will be working with, and influencing the decisions of, technical professionals (such as DevOps engineers), risk professionals and business leaders. They are expected to identify and solve complex issues, mitigate complex risks and make pragmatic decisions to balance business needs with security requirements. They will need to engage with numerous stakeholders to understand their concerns and requirements, and defend their proposals as the best, pragmatic way forward.

32. The candidate's case study should demonstrate:

- Clear awareness of the need to provide traceability between business need and security requirements;

- The ability to contextualise security recommendations and risk statements to the business need under consideration;

- The ability to support security professionals in designing secure systems and developing mitigation strategies for unusual and unique scenarios that are high risk or high complexity;

- A complete and thorough understanding of risk and risk management processes and decision making.

This can be met through:

- The application of advanced security architectures in order to mitigate security risks; and

- The ability to review system security architecture designs to ensure they mitigate identified complex or unusual security risks, whilst balancing an organisation's business requirements, e.g., reviewing complex or unusual systems to ensure that cyber-attacks are mitigated to a reasonable level, (set by the system owner) whilst balancing other factors such as user needs, costs, performance, etc.

## Summary of assessment criteria for interview

33. 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 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.

### Hypothetical workplace scenario

34. Approximately 1hr of the interview will be taken up by discussion of a hypothetical workplace scenario, designed to examine the candidate's approach to security and their ability to design and review systems. The candidate will receive the scenario at least 24 hrs before the interview. The candidate may bring notes relating to the scenario into the interview. Candidates are advised that due to the 'open ended' nature of the scenarios they should, when explaining their approach, set out the assumptions they made when dealing with the issues raised , rather than asking numerous questions of the assessors; in other words candidates should not treat the scenario as a business consultancy interview. That said, candidates may ask questions about any point (or points) which they do not fully understand and require clarification. By taking this approach, the assessors are better able to gain insight into how candidates conduct themselves as a security architect and how they approach security as well as system review and design.
35. Candidates should expect that technical topics that arise in the course of discussions around the scenario (and, in the other part of the interview, the case study/studies) will be examined in considerable detail by the assessors.

### Consultancy skills

36. In addition, candidates will also be assessed on their ability to apply their knowledge 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<br>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.<br>• 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.<br>• Understands the business context and the agenda of the stakeholders.<br>• Balance of talking and listening (70 – 30).<br>• Concerned and inquisitive. | |
| **Clear delivery and appropriate style** | • Does not organise arguments well and tends to mix key issues with trivia.<br>• Finds it difficult to adapt style to different levels of audience.<br>• Tendency to ramble and describe too much detail.<br>• May interrupt the speaker. | • Presents arguments in a clear and articulate manner selecting the appropriate level of detail to suit the audience.<br>• Good eye contact.<br>• Effective time management. | |
| **Facilitation** | • Unable to take an independent position.<br>• Unable to ensure that all voices are heard.<br>• Likely to find it difficult to manage conflicts. | • Can build consensus, manage conflict and achieve conciliation, and offer arbitration.<br>• Keen to come to an acceptable conclusion.<br>• Keen to ensure that all parties understand the other party's point of view. | |
| **Summary of overall indicators** | • Arrogance<br>• Pomposity<br>• Lack of interest | • Natural/comfortable in demeanour<br>• Confident<br>• Respectful | |

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

## Associate Cyber Professional interview: specialist knowledge assessment criteria (Security 'Architecture specialism)

### Approach

37. The interview should focus on the submitted case study examples of work conducted. Candidates should seek to demonstrate that they can apply their skills without supervision to scenarios where there is a defined framework or set of patterns to work against. An Associate Cyber Professional architect is expected to focus largely on reviewing system designs and recommending changes in concert with other members of a team. They may also provide input on the security aspects of the design of new systems. Candidates are expected to be able to technically justify the controls they recommend and why they are appropriate. The interview is expected to last approximately 1.5 hours.
38. The interview is divided into 3 distinct security architecture sections:
    - Establishing business need;
    - Reviewing architectures and identifying likely attacks;
    - Designing architectures;

39. In addition to security architecture competence, the interview will also proportionately assess a candidate's overall technical understanding and ability to assess and manage risks in business scenarios.
40. The interview should be predominantly based on a conversation about the candidate's work and submitted case studies. There are some sample questions provided which may be used as prompts for a conversation but are not mandatory. The assessors should use their judgement as to the questions that allow the candidate to best express their security architecture experience. There are no trick questions and the candidate should be invited to ask for clarification if a question is not clear, or they need it to be repeated.
41. In order to assist with the assessment and pass/fail decision making, pass and fail indicators have been provided. These indicators should be used by the assessor to moderate and gauge the answers given. There is an overall expectation that the candidate will predominantly demonstrate the pass indicators for each section. A few fail indicators are acceptable, but they should be in the minority. For either pass or fail, the assessor's judgement is paramount, and the indicators should certainly not be taken as a check list.
42. Candidates will be expected to demonstrate a reasonable understanding of technology, associated risks and the cyber security implications. A reasonable depth of understanding is expected across a range of core technologies in addition to any personal specialisms of the candidate. The assessment process should follow the broad technical disciplines applicable to the described case studies, with a few additional questions aimed at exploring breadth of technical understanding.

### The Associate Cyber Professional Standard

43. It is expected that Associate Cyber Professional practitioners will be able to demonstrate a range of experience and work on situations, some of which will have elements of complexity. They will be able to apply their technical and risk management expertise as part of a team to aid the secure design of systems.

#### Establishing business need

44. Candidates can elicit the needs of the business and elicit or derive security requirements given a set of threats and risks. They are able to identify any contradictions in business needs, security requirements and technology in a relatively well-established area where there is guidance or patterns are

available. Candidates should be able to articulate why challenges exist and highlight key areas to focus on when reviewing the security of the system.

### Reviewing architectures and identifying likely attacks

45. Given a profile of the types of threat actors a business feels they need to defend against, a candidate can evaluate a given architectural design to establish the key ways in which it could be attacked. This should include triaging potential attacks to establish the most important risks, demonstrating a robust and repeatable methodology for identification in their approach:

    - They should be able to explain how a range of attacks would likely be carried out in a with a degree of technical depth, and also be able to explain why one attack is worse than another in differing situations or with different threat profiles.

    - As well as articulating the attacks in a good level of technical detail, they should be able to explain to less technical stakeholders why particular attacks are important and how this relates to and affects the risk management for the overall system.

    - The candidate should be able to:

        - suggest pragmatic changes to the design which consider the needs of a variety of stakeholders in well-established situations;
        - articulate why the changes provide the best balance between managing the security risks and needs of other stakeholders, not least the users;
        - articulate what residual risks exist even with the proposed changes; and
        - articulate why, in some situations, an appropriate level of security cannot be achieved.

    - Unless a candidate is demonstrably a deep expert in a particular technical specialism (e.g. web technology), it is important that they can do all of this over a range of technical areas. Such areas might include web, operational technology, enterprise systems and high threat environments. It is expected that candidates will take an interest in emerging technology, or a specific area of technology and be able to articulate key security challenges or opportunities in their area.

### Designing architectures

46. Candidates should be able to contribute to the design of new architectures as part of a wider team. This may be working on novel designs with a more senior architect or owning parts of a design in a well established area. They should demonstrate their ability to select the correct security controls and integrate them appropriately into the architecture.

47. The candidate should be able to demonstrate how they:

- assessed the risks;
- evaluated potential technical solutions;
- designed elements of an overall architecture; and
- established key residual risks and how to manage them.

48. Candidates should show a consistent approach to ensuring that appropriate assurance activities are followed for both their designs and the overall system they are working on. They should also demonstrate that they consider the complete range of risk management activities across the life cycle of the system. This includes user behaviour, operations, management and monitoring

## 49. Certified Cyber Professional interview: specialist knowledge assessment criteria (security architecture specialism)

50. Certified Cyber Professional security architect is considered a "leading light" in the architecture community who can review or design the security of any system without supervision in areas they are not familiar with. They should be able to design the security of new and complex systems using a range of technology, based on a deep technical background and in-depth knowledge and experience of risk management. Candidates are expected to be able to technically justify the controls they recommend and why they are appropriate.
51. It is expected that a Certified Cyber Professional architect will be able to work without supervision (although following a robust quality control process) in the design of organisationally important systems which have a complex set of security risks using new forms of technology. Whilst doing this, they will be working with and influencing the decisions of technical professionals (such as DevOps engineers), risk professionals and business leaders.
52. They are expected to identify and solve complex issues, mitigate complex risks and make pragmatic decisions to balance business needs with security requirements. They will need to engage with numerous stakeholders to understand their concerns and requirements, and defend their proposals as the best, pragmatic way forward.

### Approach

53. The interview should focus on the submitted case study. However, the supporting examples should also be discussed to ensure that there is breadth to the candidate's experience. Whilst it is natural that a candidate is likely to have a particular technical specialism for Certified Cyber Professional level security architecture, they must be able to demonstrate the ability to apply the security architecture skillset to a range of scenarios and technologies. The focus of Certified Cyber Professional level is on the ability to apply skills to scenarios without precedent, either due to complex risk management, or use of technology. The interview is expected to last approximately 2 hours.

54. The interview is divided into 4 distinct security architecture sections:

    - Establishing business need;
    - Reviewing architectures and identifying likely attacks;
    - Designing novel architectures;
    - Thought leadership.

55. In addition to security architecture competence, the interview will also proportionately assess a candidate's Overall technical understanding and ability to build a robust risk management approach from first principles in an area with no established "case law."

56. The interview should be predominantly based on a conversation about the candidate's work on the submitted case study and additional supporting examples. There are some sample questions provided below (see Appendix E).

## The Certified Professional Standard

57. It is expected that Certified Cyber Professionals will be able to demonstrate a range of experience and work on situations with complicated architectural scope. They will be able to apply their expertise in difficult or unusual circumstances based upon the interplay of technical knowledge and the fundamental principles of risk management.

### Establishing business need

58. The candidate can elicit complicated, non-obvious security requirements that are directed by the overall business and user needs. The mapping between business needs, security requirements and the technology will be non-trivial to resolve. We would expect them to be able to identify the key contradictions in business needs, security requirements and technology. They should be able to articulate why challenges exist, such as technology not being designed for the specific use case. This is likely to involve non-obvious technicalities such as subtleties of protocols or cryptographic architectures. At Certified Cyber Professional level, we would expect there to be no pre-existing guidance or patterns which can be applied to solve the problem. They should also be able to articulate the key areas that need to be focussed on to design a solution which maintains an acceptable balance of business needs, security requirements and technical complexity / cost.

### Reviewing architectures and identifying likely attacks

59. Given a profile of the types of threat actors a business feels they need to defend against, the candidate should:
    - Be able to evaluate a given architectural design to establish the key ways in which it could be attacked. This should include triaging potential attacks to establish the most important risks.
- Demonstrate a robust and repeatable methodology for identifying potential attacks and be able to explain how particular attacks would likely be carried out in a reasonable level of technical depth.
- Be able to explain why one attack is worse than another in differing situations or with different threat profiles.
- As well as articulating the attacks in a good level of technical detail, they should be able to:
- Explain to less technical stakeholders why particular attacks are important and how it relates to and effects the risk management for the overall system.
- Suggest pragmatic changes to the design which take into account the needs of a variety of stakeholders.
- Articulate why the changes provide the best balance between managing the security risks and needs of other stakeholders, not least the users.
- Articulate what residual risks exist even with the proposed changes and explain why, in some situations, an appropriate level of security cannot be achieved.

60. Unless the candidate is demonstrably a deep expert in a particular technical specialism (e.g. web technology), it is important that they can do all of this over a range of technical areas. Some areas might include web, operational technology, enterprise systems and high threat environments.

### Designing novel architectures

61. The candidate should be able to design architectures from scratch given a use case, set of business needs, threats and a risk appetite. They should be able to show where they have designed an architecture which is in some way without precedent; i.e. it is not a solved problem with patterns available. This may be due to the use of new technology or an unusual set of business needs or threats.
62. The candidate should be able to demonstrate how they assessed the risks, evaluated potential technical solutions, designed an overall architecture and established key residual risks and how to manage them. This can be done individually or as part of a larger team, as long as the candidate can show that they provided key technical security input and can work as part of a wider security team. They should discuss how they seek the support of subject matter experts for areas requiring deeper knowledge, such as cryptography.
63. The candidate should show a consistent approach to ensuring that appropriate assurance activities are followed for both their designs and the overall system they are working on. They should also demonstrate that they consider the complete range of risk management activities across the life cycle of the system. This includes user behaviour, operations, management and monitoring. As part of this, they should be able to clearly articulate the importance of each different aspect of risk management and demonstrate experience of defining the security for these activities such as defining monitoring controls, management plans and system operating procedures.

### Thought Leadership

64. The candidate can demonstrate that they further the security architecture profession through contributing novel ideas to the community, developing other architects and enhancing the understanding of secure design / risk management across wider technology profession. As part of this it is expected that an architect, whilst well rounded, will have particular specialisms such as operation technology, enterprise networks and web engineering. At Certified Cyber Professional level, it is expected that they are regarded as an expert in the security of these technologies by their local community.

## Revalidation process

65. 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.
66. 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.
67. 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[8]
- 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

68. 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.

[8] 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

In 2019 [9]I was engaged by a London-based wealth management company to review their existing IT systems and digital business use cases, and define a security architecture as part of their IT refresh and uplift programme[10]. The company has approximately 75 professional advisors managing circa £10 billion assets for their clients, with a total company employee headcount of approximately 100.

**Establishing the business need and defining security requirements**

Primary digital business use cases included accessing online trading platforms, and email and SaaS platforms for client correspondence and portfolio management. The various data repositories hosted significant quantities of sensitive personal and financial data. The CEO instructed me that the company needed to exploit digital access methods and communications (including mobile devices) to maintain and expand the company's client base. At the same time they needed to be risk averse to a data breach via cyber methods. This was because according to a risk assessment commissioned by the CEO, a breach would severely impact client retention and new client onboarding, in-turn severely impacting the company and their profit[11].

As part of initial discovery and scoping activities, I worked closely with three key stakeholders to ensure I comprehensively understood the business and user need. These were the CEO and senior leadership team, Solution Architect and Compliance Executive. I proposed technology landscape and legislative / regulatory constraints. This discovery and scoping exercise enabled me to define a set of security requirements which provided a 'golden thread' through the consultancy activity with full traceability from business. s need through to the implementation and maintenance of security controls[12].

**Reviewing the proposed technology uplift and defining the security architecture**

A primary driver of instigating the technology refresh and uplift for the company was the significant underperformance of the existing managed service provider against contractual service levels. This included a weak security posture which had enabled a compromise using SocGholish malware with suspected attribution to the EvilCorp ransomware group. A subsequent investigation found a lack of uniformly applied security controls, e.g., server and end user device hardening, anti-virus software etc.

The company engaged a solution architect to design a corporate IT system which did not use the managed service provider's data centre to host servers and applications. It would instead use a new managed service provider (to be chosen by a competitive process) to manage and deliver all IT services going forward. At a high level, the solution architect designed a system as follows:

- All servers and applications to be migrated from the managed service provider's data centre to Microsoft Azure UK data centres.
- Existing SaaS platforms for client correspondence and portfolio management continue to be used.
- End user access via BYOD mobile phones and laptops used in the office or remotely.

My next task was to review the solution architect's design and define the security architecture and technical security controls to ensure the new IT system was resilient to cyber compromise as per the CEO's risk averse stance, while also supporting the user access methods and service requirements.

To define security architecture, I used the NCSC 10 Steps to Cyber Security framework. The reason I chose this as opposed to other frameworks which may be used to define a security posture and controls (e.g. NIST 800-53, SABSA, etc.) is because the NCSC 10 Steps to Cyber Security lend themselves well to demonstrating cyber maturity against a reasonable set of categories to senior stakeholders. The 10 Steps framework also has clear linkage to a concise and cohesive set of design patterns and guidance to ensure comprehensive coverage of security controls.

---

[9] Case study within the last 3 years

[10] Role within case study appropriate for Level 2 security architecture specialism

[11] Sufficient size, value, complexity and strategic importance

[12] DER 1 Traceability between business need and security requirements

A non-exhaustive list of highlights from my design review and application of the 10 Steps were[13]:

- I ensured the **Azure and O365 platform** had best practice applied in all areas e.g. network segregation using NSGs to prevent lateral pivoting of malware, MFA for normal users (using conditional access) and privileged users (using an authenticator app) to mitigate common password attacks affecting cloud services e.g., password spraying or re-use of compromised credentials. I also applied Microsoft security configuration baselines to mitigate the potential of malware by privilege escalation, etc.
- I reviewed the existing **SaaS** provider technical security posture using the NCSC SaaS principles and financial services' regulatory requirements. I ensured any weaknesses that could be exploited in the context of their use were escalated to the corporate security risk register for mitigation and management.
- I advised application of the **end user device** security guidance for Windows 10 laptops. This ensured that a robust model was in place to mitigate attacks associated with remote working e.g. PitM, by using an IPSec VPN. I minimised the impact of malware by using application white-listing, and ensuring all traffic in and out of the laptop would traverse the company's boundary security controls.
- I overlayed technical **malware mitigation** security controls onto the solution architect's design with a blend of signature and AI detection using the Microsoft cloud-driven suite. This included Microsoft 365 Defender and Microsoft Defender ATP, and a virtual network intrusion detection device with threat intelligence and supporting custom IOCs to protect and detect endpoints beaconing outbound to malicious C2 networks. These malware mitigation controls were complemented by the platform and EUD security controls stated above to limit the efficacy of a cyber-attack, and robust logging and monitoring were put in place to alert and respond accordingly.
- I defined a **security logging and monitoring** posture using NCSC published guidance. The key drivers were 1) ensure suitable log capture and retention were in place to meet financial services' regulatory compliance and incident response requirements, 2) provide an intuitive monitoring console and timely alerting mechanism, and 3) input security requirements into the competition process for the new managed service provider to ensure procedural aspects of security monitoring were in place, e.g., sufficient SOC triage and response processes. The technical solution I defined to underpin this was the Azure Sentinel SIEM. The rationale was that this seamlessly leveraged the existing platform security data sources, e.g., Microsoft Defender ATP, and additionally other Syslog devices such as the virtual IPS device, thus providing a coherent capture, alerting and analysis toolset. In detailed technical workshops with relevant SMEs, using my knowledge of the architecture, I conducted attack tree modelling to identify the most likely attacks. I then worked with Cyber Engineers to create monitoring rules for these attacks and ensured appropriate logs were collected.
- **BYOD** was a mandated user need, or more specifically when I dug deeper I identified the requirement for access from employee Apple and Android phones to corporate email and a single business app for one of the SaaS applications. I reviewed a number of Mobile Device / Application Management technologies that may meet the requirement including MobileIron and Cisco Meraki, eventually choosing Microsoft InTune which integrated well with the existing Microsoft infrastructure services. It enabled employees to use their personal mobile phones without being enrolled and fully managed, but enabled the single business app and corporate email as policy managed applications e.g. PIN protected and data-encrypted, to mitigate data loss outside of the app. I explained to the CEO that this did not mitigate all risks associated with BYOD working e.g. a jailbroken device or compromised credentials that may result in an undetected malicious cyber event.
- BYOD API Restrictions - The CEO was content with the above for most uses, however was worried of the risk of a compromised BYOD device being used to move clients' money. The SaaS platform published their full web service API. From reviewing this, I noticed the MoveMoney REST endpoint supported a flag in the request which either immediately actioned the transaction or added it to an approval workflow. For audit retention purposes independent of the SaaS provider, I had already

[13] Sub- paragraphs demonstrate evidence against:

DER 2 - Review architectures and identify likely attacks for simple or obvious security requirements for highly standardised use cases, using well established guidance.

DER 3 – The ability to provide security architecture designs to address standard security needs.

DER 5 - The ability to meaningfully describe straight-forward security concepts and their business applicability.

recommended a TLS offloader in Azure before the traffic was sent to the SaaS application. I therefore designed an **Azure Function** which triggered on this specific REST endpoint. It inspected the client certificate connecting. If the certificate was issued from the BYOD sub-CA, it forced the addition of the review workflow flag into the POST request, adding it to a queue only accessible to internal (non BYOD) users. This resolved the issue, at the cost that the API must be monitored for upcoming changes which may require the Azure Function to be updated[14].

Alongside using the 10 Steps to define the security controls, I also used the MITRE ATT&CK framework to map applicable adversary TTPs to the security controls I had put in place. This ensured that I related likely adversary behaviours at a detailed level to the security architecture, and could tailor / augment controls accordingly e.g. strengthening server and end user device application allow-listing based on the tools identified in the Tactic à Execution area such as PowerShell etc[15].

For assurance, I ensured my security architecture was peer reviewed by a SQEP colleague, and also recommended a penetration test to ensure the efficacy of the implementation and configuration. I defined the scope of this pentest to include specific areas based on the attack tree performed earlier. This penetration test was executed, and I prioritised the remediation plan for the company to ensure the vulnerability posture of the system was at an acceptable level. I also recommended Cyber incident response insurance which was lacking and had therefore led to significant additional cost in forensic investigation and remediation when the previous compromise had occurred[16].

**Customer Benefit**

I encouraged and secured the significant investment from the company by detailing my structured approach and benefits at a meeting with the CEO and other key board members such as the CFO. The main thrust of my approach was to detail how each of the controls would have prevented impact associated with the previous compromise. For example, the security monitoring controls I put in place would have detected the attack as it happened, and the logging would have provided better support for forensic investigation. The application allow-listing would have prevented the malware from executing and alerted the SOC. The virtual IPS device with IOCs implemented would have blocked the C2 attempts[17].

The outcome was that the Security architecture and controls I proposed were given the appropriate investment and the CEO was content that the business could exploit modern technologies while at the same time having adequate protection from cyber related business impacts.

[14] DER 6 - The ability to contextualise security recommendations and risk statements to the business need under consideration

DER 8 - An understanding of the fundamentals of risk and risk management processes and decision making.

[15] DER 2 - Review architectures and identify likely attacks for simple or obvious security requirements for highly standardised use cases, using well established guidance.

[16] DER 4 – Awareness of limitations and scope for what advice can be given and when to draw on others expertise.

[17] DER 6 - The ability to contextualise security recommendations and risk statements to the business need under consideration

## Appendix A: Exemplar case studies: Certified Cyber Professional

In 2020[18] I was engaged by a large public sector organisation (hereafter 'the organisation' or 'the Department) to review their proposed architecture for their Strategic Interoperability Services Programme (SISP) and define an appropriate security architecture for this major programme to be delivered over a 3 year timeframe and be fit for purpose for the next 10 years[19]. The aim of SISP was to replace the Department's existing interoperability services with other nations, industry partners and OGDs at the Secret classification, with a value circa. £500 million[20].

**Establishing the business need**

Existing organisational interoperability services were viewed by the user as providing an inadequate experience, specifically the high-assurance cross-domain security controls were constraining the ability of the end user to work effectively across a variety of common interoperability use cases, e.g. email, chat, video conferencing and content collaboration with external organisations. Some of this poor user experience led to significant consequences e.g. lack of situational awareness in operational situations, and the inability to communicate effectively and in a timely manner on time-critical tasks. Additionally, a requirement of the SISP programme was also to reduce the through-life cost of delivering and maintaining interoperability services by using modern technologies and approaches in a secure manner e.g. virtualisation, orchestration and elasticity.

As discussed in more detail throughout this case study, the capability and motivation of threat actors associated with some of the external partners and systems the organisation was required to collaborate with posed , as did the 'averse' risk appetite of the Department to threat actor persistence and compromise of assets at the Secret classification.

**Defining the Security Requirements**

Having established the high-level programme mandates, I set about working closely with the technical design team to understand the proposed platform and cross-domain services that were put forward to deliver the richer user experience at a reduced through-life cost. This enabled me to get a high-level view of how the technical design team were approaching the user and system requirements, and how my security architecture would need to complement / support or even challenge this approach. Alongside this, I sought a threat brief from the Cyber organisation specific to the external systems and services that would be delivered to interoperate with these external partners.

The next step was to feed all of these factors into a risk assessment which I conducted using the NIST 800-30 methodology, which also defined the TTPs of potential threat actors, helping me to shape my thinking around strength of security controls, which I coupled with the ISO27001 control set to define a set of coherent security requirements. I chose the technical areas of the ISO27001 control set rather than the NIST control framework since from previous use I viewed the NIST framework as overly-focused on standard use cases, whereas ISO27001 technical control areas gave me the flexibility I needed to define specific security requirements for complex cross-domain services. For example, I used the 'A12.2. Controls against Malware' to define security requirements specific to the cross-domain service and external partner at a granular level. This included types and efficacy of content transformation and verification checks, e.g. hardware enforced, and unidirectional flow control, e.g. firewall or optical / electrical data diode[21].

The culmination of this extensive groundwork enabled me to define a set of security requirements which provided a 'golden thread' with full traceability from business need through to the implementation and maintenance of security controls .

**Reviewing the proposed technical architecture and defining the security architecture**

---

[18] Case study within the last 3 years

[19] Role within case study appropriate for Level 3 security architecture specialism

[20] Sufficient size, value, complexity and strategic importance

[21] DER 5 The ability to meaningfully describe more complex security concepts and their business applicability

DER 8 - An understanding of the fundamentals of risk and risk management processes and decision making.

DER 1 Traceability between business need and security requirements

At a high level, the technical architecture presented to me by the organisation's design team mapped onto the user and system requirements as shown in the diagram below. Additionally, it was explained to me that the solution must be made of COTS hardware and software – the Department had system integrator skills but did not have the appetite to generate bespoke code or hardware blueprints.

Some of the key challenges in defining a suitable technical security posture that provided richer services to the user within the risk appetite and cost envelope, and how I addressed them, are described below. The organisation's proposed architecture and my security architecture overlaid on this are shown in diagrams 1 and 2 below[22]:

- The **CDS Security Controls** suggested were generic and did not correlate to the threat actor capability or motivation of the specific external partner. Therefore, I used the NCSC's data import and export patterns to define cross domain service security controls commensurate to the threat brief for each external partner. For example, one connection was to another government department. This OGD had a robust and well understood security posture. Onward connectivity enabled bidirectional services with rich content sharing, and security controls focused on helping the user to not inadvertently release inappropriate information e.g. sensitive word checking, release label checking etc. Conversely, for an email service to a nation whose connecting IT system was known to be weak and potentially used as a platform by a motivated and capable threat actor, I defined security controls with:
    - File format transformation to disrupt malware – specifically transforming to an XML-like format then taking only required content for onward transmission.
    - Hardware enforced protocol break, unidirectional flow and syntactic content verification checking. Implementing these security controls in hardware ensured a minimal vulnerability footprint and attack surface.
    - Software enforced semantic verification checks as part of the transform process back to the native file format.
- I viewed the **Mgt Terminals** hosted in the collaboration and infrastructure services zone directly managing the CDS Zone as presenting an opportunity for a compromised management terminal to attack a CDS service(s). This is because the aforementioned motivated and capable threat actor consuming services / connected to this zone could exploit a vulnerability e.g. in the hypervisor or email server and pivot laterally to the management terminals. Therefore, I defined separate management zones to ensure management terminals could not be used to bypass the data path. A similar issue was presented by the SIEM, so I used guidance in the NCSC Architectural Pattern 1 to define a security monitoring posture whereby the SIEM could not be used as a bypass channel by the threat actor resident on external partner networks[23]. Both of these introduced additional cost and complexity into the system which I presented to the programme manager, with subsequent briefing to the project sponsor, explaining that in the context of the threat brief the previous solution would be significantly outside of their risk tolerance were they to proceed with it.
- The **Update Services** (security patches, functional patches etc.) hosted in the collaboration and infrastructure services zone were directly connected to the internet. This concerned me since, amongst other things, it created an additional persistent repository and connection for Secret data exfiltration (both organisation and partner data), and also an ingress path for malware and resulting C2, with the only control proposed being the update services server anti-virus signatures. Therefore, I separated the update services from the collaboration and infrastructure services zone by using a separate server with a hypervisor configured for non-persistence i.e. newly-orchestrated OS image after the scheduled task, to download and forward completed updates. I presented hardware enforced protocol breaks and data diodes for onwards transfer to the CDS and collaboration and infrastructure services zone. I briefed the programme manager and sponsor that while this provided very good protection against update services being used for C2 and data exfiltration, the content could not be verified as known good, and there was a reliance on supply chain security controls to provide greater mitigation, but ultimately using COTS products meant malware may be delivered via a supplier intentionally or inadvertently. The CDS SEFs were updated via media directly from the supplier, with the code and development practices being assured to a high level via an appropriate scheme e.g. CAPS, CTAS etc.

[22] DER 2 The ability to review architectures and identify likely attacks with complex security requirements for non-standardised use cases, using well established or novel guidance.

[23] DER 6 - The ability to contextualise security recommendations and risk statements to the business need under consideration

- The threat brief suggested that threat actors resident on some of the external partner networks may be motivated and capable of **breaking out of their virtual tenancy** in the collaboration and infrastructure services zone, and compromise the confidentiality of another tenant's Secret data e.g. an OGD or industry partner. Therefore, I recommended in this case that physically separate collaboration and infrastructure services should be used for these external partners. Since this recommendation impacted the cost-model and use of modern approaches such as elasticity to be exploited, this was escalated to the SIRO where I explained that virtualisation software separation techniques could not be relied upon in this scenario, and the SIRO was content since the impact of compromise would cause significant reputational damage to the organisation[24].

For assurance, I ensured my security architecture was peer reviewed by a SQEP colleague and further by NCSC SMEs, and also recommended a penetration test to ensure the efficacy of the implementation and configuration[25]. Cross-domain SEFs were evaluated using the output of reports from the NCSC CDS Pilot scheme. This penetration test was executed, and I prioritised the remediation plan for the organisation to ensure the vulnerability posture of the system was at an acceptable level.

**Customer Benefit**

The outcome was that the Security architecture and controls I proposed were given the appropriate investment, and the sponsor and SIRO were content that an appropriate balance had been met between the security architecture and programme mandates to enhance the user experience, exploiting modern technologies and methods, and reducing the costs of the organisation's interoperability services through-life.

[24] DER 5 The ability to meaningfully describe more complex security concepts and their business applicability

[25] DER 4 – Awareness of limitations and scope for what advice can be given and when to draw on others expertise.

**Diagram 1: Proposed Technical Architecture**

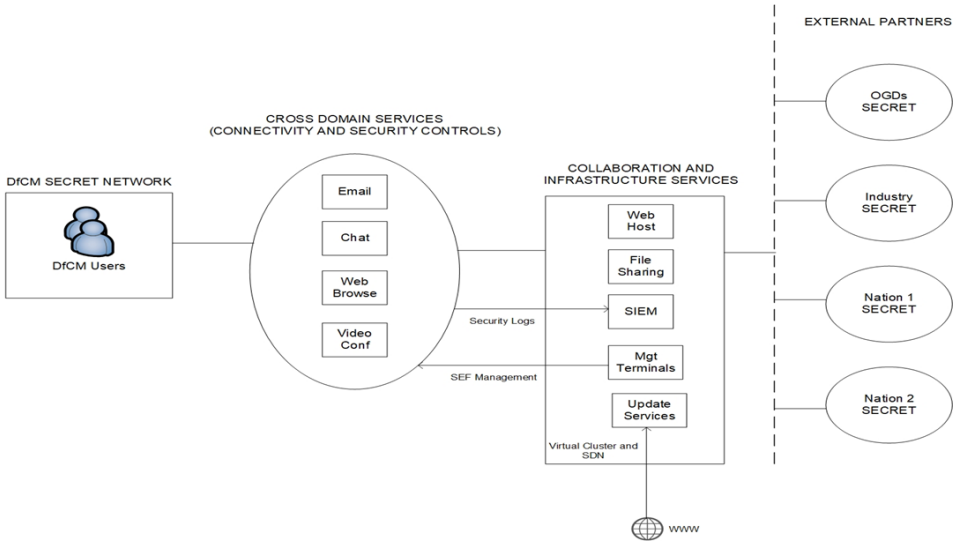
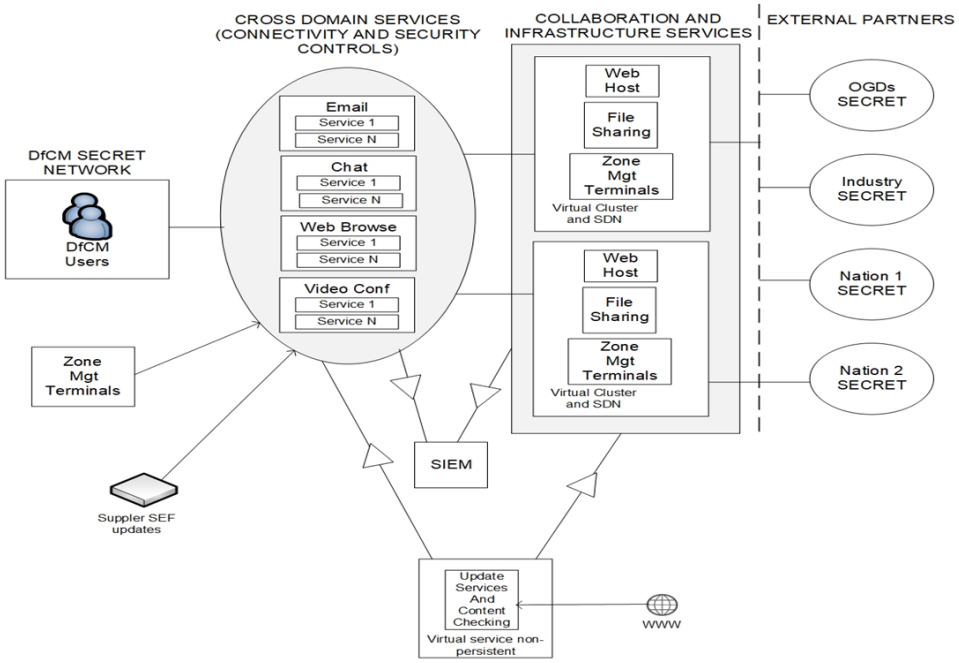


**Diagram 2: Updated Technical Architecture with Security Architecture Overlaid[26]**




[26] DER 3 - The ability to provide advanced security architecture designs to address unusual or complex security needs

## Appendix B: Pro forma for the assessment of case studies: Associate Cyber Professional

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), who should be able to confirm that the case study accurately describes the work undertaken by the applicant 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 3 years? | | |
| Were the role and level of responsibility of the applicant in this case study relevant to the level of 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 Clear awareness of the need to provide traceability between business need and security requirements. | | |
| No.2 The ability to review architectures and identify likely attacks for simple or obvious security requirements for highly standardised use cases, using well established guidance. | | |
| No.3 The ability to provide security architecture designs to address standard security needs. Advice could be written or verbal. | | |
| No.4 An awareness of limitations and scope for what advice can be given and when to draw on others' expertise. | | |
| No.5 The ability to meaningfully describe straight-forward security concepts and their business applicability. | | |
| No.6 The ability to contextualise security recommendations and risk statements to the business need under consideration. | | |
| No.7 The ability to support security professionals in designing secure systems and developing mitigation strategies for relatively common and well understood scenarios. | | |
| No.8 An understanding of the fundamentals of risk and risk management processes and decision making. | | |

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

## Appendix B: Pro forma for the assessment of case studies: Certified Cyber Professional

| Requirement | Confirmed Yes/No | Comments |
|---|---|---|
| Does the Case Study describe work carried out within the last 3 years? | | |
| Were the role and level of responsibility of the applicant in this case study relevant to the level of 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 Clear awareness of the need to provide traceability between business need and security requirements. | | |
| No.2 The ability to review architectures and identify likely attacks with complex security requirements for non-standardised use cases. While this may use some well-established guidance, it is expected that at this level there will be novel elements outside existing guidance. (Could be contentious and need persuasive techniques to implement.) | | |
| No.3 The ability to provide advanced security architecture designs to address unusual or complex security needs. It is expected that the solutions are novel and cannot just be implementations following standard patterns. Advice could be written or verbal. | | |
| No.4 An awareness of limitations and scope for what advice can be given and when to draw on others' expertise. | | |
| No.5 The ability to meaningfully describe more complex security concepts and their business applicability. | | |
| No.6 The ability to contextualise security recommendations and risk statements to the business need under consideration. | | |
| No.7 The ability to support security professionals in designing secure systems and developing mitigation strategies for | | |

| | | |
|---|---|---|
| unusual and unique scenarios that are high risk or high complexity. | | |
| No. 8 A complete and thorough understanding of risk and risk management processes and decision making. | | |

## 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.<br>• 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.<br>• Understands the business context and the agenda of the stakeholders.<br>• Balance of talking and listening (70 – 30).<br>• Concerned and inquisitive. | |
| **Clear delivery and appropriate style** | • Does not organise arguments well and tends to mix key issues with trivia.<br>• Finds it difficult to adapt style to different levels of audience.<br>• Tendency to ramble and describe too much detail.<br>• May interrupt the speaker. | • Presents arguments in a clear and articulate manner selecting the appropriate level of detail to suit the audience.<br>• Good eye contact.<br>• Effective time management. | |
| **Facilitation** | • Unable to take an independent position.<br>• Unable to ensure that all voices are heard.<br>• Likely to find it difficult to manage conflicts. | • Is able to build consensus, manage conflict and achieve conciliation, and offer arbitration.<br>• Keen to come to an acceptable conclusion.<br>• Keen to ensure that all parties understand the other party's point of view. | |
| **Summary of overall indicators** | • Arrogance<br>• Pomposity<br>• Grandiose<br>• Lack of interest | • Natural/comfortable in demeanour<br>• Confident<br>• 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** | **Score** | **Comments** |
| • Evidence of how business needs are systematically determined, gathered and understood, including an understanding of high-level mission objectives<br>• Understands and uses appropriate methods and techniques for establishing business need<br>• Can demonstrate elicitation of non-obvious security needs.<br>• Understands and can articulate how security requirements directly support the needs of the business<br>• Demonstrates an ability to balance business needs and security<br>• Can articulate the "crux" challenges for delivering an appropriately secure system that meets business needs | • Focusses on simple C, I and A requirements without business context<br>• Cannot demonstrate how the business needs were investigated or taken into account (even if not done by the candidate themselves)<br>• Shows a lack of understanding of a standardised way of determining security requirements<br>• Unable to demonstrate the ability to map or explain complicated security requirements<br>• Unable to explain why particular combinations of needs, threats and technical solutions are challenging | [explore the process of establishing security requirements based upon business need in the provided case study]<br>Describe a situation where there was a tension between business needs, risks and technology<br>• How did you identify this?<br>• What did you do?<br>• What was the outcome?<br>Describe a situation where there was an actual or perceived conflict between security requirements and business need<br>• How was the conflict identified?<br>• How did you help in resolving the conflict?<br>• What was the outcome?<br>Describe a situation where the customer didn't agree with your assessment of security need.<br>• What was the basis of the disagreement?<br>• How did you respond? Were you able to come to an agreement? | | |

| 2. Reviewing architectures and identifying likely attacks – 40-45 minutes | | | | |
|---|---|---|---|---|
| Pass indicators | Fail indicators | Sample questions | Score | Comments |
| • Can describe how to assess how a system can be attacked given a threat profile<br>• Can describe how they assess which attacks are the highest risk and therefore prioritise remediations<br>• Can demonstrate assessing the security of a system across a range of sectors and types of technology<br>• Can explain how particular attacks would be carried out (technically)<br>• Can explain attacks in non-technical language and describe how it affects the overall system's risk profile<br>• Can demonstrate designing pragmatic solutions to security challenges which balance security and business needs<br>• Can defend why their suggested solution to an attack is the best approach<br>• Can demonstrate that they have an active interest in technology and the security implications | • Cannot demonstrate a robust and repeatable methodology for assessing systems<br>• Cannot justify why specific risks are more important than others for a specific system<br>• Does not demonstrate experience of reviewing systems across a range of technologies or sectors<br>• Cannot explain in a reasonable level of technical depth how any identified attacks would be carried out<br>• Cannot relate a technical attack to a non-technical person<br>• Suggests technical solutions which only consider security and ignore business or user needs<br>• Cannot justify or defend their suggested architectural change<br>• Does not acknowledge residual risks | Describe how you reviewed the security of a system:<br>• What process did you follow?<br>• How did you identify the risks?<br>• How did you prioritise risks?<br>Thinking of one of the risks, how would the attack be realised? [expect technical explanation]<br>• How would you explain this to a non-technical person?<br>• Why is this more / less important than other risks?<br>• What impact does this have on the overall system design?<br>What changes did you recommend?<br>• How does this balance security, business and user needs?<br>• What were the residual risks?<br>Pick a few other candidate case studies to assess the candidate's breath of experience and skills. | | |

| 3. Designing architectures – 15-25 minutes | | | | |
|---|---|---|---|---|
| Pass indicators | Fail indicators | Sample questions | Score | Comments |
| • Has contributed to the security design of a system, working as a wider team<br>• Focuses on designing security that is "good enough" to enable the business<br>• Considers how their areas of responsibility feed into the overall security and risk management of the system<br>• Can apply design skills to a range of technical areas (e.g. web, enterprise, operational technology)<br>• Can demonstrate their designs are realistic and implementable rather than simply academically interesting<br>• Can justify every element of the design against overall requirements given to them<br>• Utilises subject matter experts appropriately<br>• Works as part of a team to arrive at the best solution<br>• Can justify their designs to a range of technical and non-technical stakeholders<br>• Acknowledges and manages residual risks<br>• Understands different sources and approaches to gaining assurance. This includes a clear understanding of the benefits and limitations of different assurance techniques<br>• Applies sensible mitigations where formal assurance cannot be obtained | • Cannot apply published patterns and guidance to enable the secure design of a system<br>• Cannot demonstrate how their designs mitigate the risks<br>• Cannot explain why each element of their design is required and how it contributes to the overall system<br>• Does not consider the wider system and its objectives in the scope of their design<br>• Does not demonstrate understanding the need for independent assurance<br>• Cannot explain how different approaches to products, implementation and operational assurance can be effective<br>• Focuses on specific aspects of assurance such as certifications rather than determining overall confidence at a system level | • Describe a system where you have designed elements of its security architecture<br>• How did you decide on the type of solution required?<br>• Describe your technical solution<br>• How does your solution manage the risks?<br>• Why is this the best way to meet the business need?<br>• How did you ensure your design contributed to the overall system security?<br>• What was the outcome of this design?<br>• What are the residual risks and how are they managed?<br>• Pick a few other candidate case studies to assess the candidate's breath of design skills.<br>• Can you provide some examples of assurance activities and explain what the value of these were? | | |

## 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** | **Score** | **Comments** |
| • Evidence of how business needs are systematically determined, gathered and understood, including an understanding of high-level mission objectives<br>• Understands and uses appropriate methods and techniques for establishing business need<br>• 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<br>• Understands and can articulate how security requirements directly support the needs of the business<br>• Demonstrates an ability to balance business needs and security<br>• Can explain technical subtleties which make devising a solution for the specific use case challenging<br>• Can articulate the "crux" challenges for delivering an appropriately secure system that meets business needs | • Focusses on simple C, I and A requirements without business context<br>• Determines business need from only a small set of stakeholders such as security, or developers<br>• Lack of evidence that the business was effectively consulted or considered<br>• Shows a lack of understanding of standardised way of determining security requirements<br>• Unable to demonstrate the ability to map or explain complicated security requirements<br>• Unable to explain why particular combinations of needs, threats and technical solutions are challenging<br>• States that business security needs are based purely on policy as opposed to understanding the threat / risk | • [explore the process of establishing security requirements based upon business need in the provided case study]<br>• Describe a situation where there was a complex interplay between business needs, risks and technology<br>• How did you identify this?<br>• What was the complexity?<br>• What did you do?<br>• What was the outcome?<br>• Describe a situation where there was an actual or perceived conflict between security requirements and business need<br>• How was the conflict identified?<br>• What was your approach to resolving the conflict?<br>• What was the outcome?<br>• Describe a situation where the customer didn't agree with your assessment of security need.<br>• What was the basis of the disagreement? | | |

| | | | | |
|---|---|---|---|---|
| | | • How did you respond?<br>• Were you able to come to an agreement? | | |

| 2. Reviewing architectures and identifying likely attacks – 30-40 minutes | | | | |
|---|---|---|---|---|
| Pass indicators | Fail indicators | Sample questions | Score | Comments |
| • Can describe how to assess how a system can be attacked given a threat profile<br>• Can describe how they assess which attacks are the highest risk and therefore prioritise remediations<br>• Can demonstrate assessing the security of a system across a range of sectors and types of technology<br>• Can explain how particular attacks would be carried out (technically)<br>• Can explain attacks in non-technical language and describe how it affects the overall system's risk profile<br>• Can demonstrate designing pragmatic solutions to security challenges which balance security and business needs<br>• Can defend why their suggested solution to an attack is the best approach<br>• In their answers, is able to go into a good level of technical depth and clearly understands the intricate technical details as well as how those technicalities relates to risk | • Cannot demonstrate a robust, repeatable methodology for assessing systems<br>• Cannot justify why specific risks are more important than others for a specific system<br>• Does not demonstrate experience of reviewing systems across a range of technologies or sectors<br>• Cannot explain in a reasonable level of technical depth how any identified attacks would be carried out<br>• Cannot relate a technical attack to a non-technical person<br>• Suggests technical solutions which only consider security and ignore business or user needs<br>• Cannot justify or defend their suggested architectural change<br>• Does not acknowledge residual risks<br>• Cannot demonstrate working with designs or risk management which are complex and novel<br>• Answers lack technical detail or concern fairly standard systems | • Describe how you reviewed the security of a system:<br>• What process did you follow?<br>• How did you identify the risks?<br>• How did you prioritise risks?<br>• Thinking of one of the risks, how would the attack be realised? [**expect technical explanation**]<br>• How would you explain this to a non-technical person?<br>• Why is this more / less important than other risks?<br>• What impact does this have on the overall system design?<br>• What changes did you recommend?<br>• How does this balance security, business and user needs?<br>• What were the residual risks?<br>• Pick a few other candidate case studies to assess the candidate's breath of experience and skills. | | |

| 3. Designing novel architectures – 40 to 45 minutes | | | | |
|---|---|---|---|---|
| Pass indicators | Fail indicators | Sample questions | Score | Comments |
| • Designed systems (or part thereof) where the security and risk management is without precedent<br>• Focusses on designing security that is "good enough" to enable the business<br>• Considers overall system objective and threats in designing solution or component; the "big picture."<br>• Can apply design skills to a range of technical areas (e.g. web, enterprise, operational technology)<br>• Can demonstrate their designs are realistic and implementable rather than academically interesting<br>• Can justify every element of the design against overall requirements and risk management plan in a good level of technical detail<br>• Utilises subject matter experts appropriately<br>• Works as part of a team to arrive at the best solution<br>• Can justify their designs to a range of technical and non-technical stakeholders<br>• Acknowledges and manages residual risks<br>• Understands different sources and approaches to gaining assurance. This includes a clear understanding of the benefits and limitations of different assurance techniques<br>• Tailors assurance to the desired security properties of each component<br>• Applies sensible mitigations where formal assurance cannot be obtained<br>• Can explain to risk owners why sometimes formal assurance is less important than the overall architecture and risk management | • Designs overly complex or costly solutions where the security cannot be justified<br>• Is a "lone wolf," or does not consider other's viewpoints or suggestions<br>• Cannot demonstrate work on systems where there is no pre-existing guidance or patterns to follow<br>• Has not involved, or has ignored views of key stakeholders<br>• Cannot demonstrate how their designs mitigate the risks<br>• Does not consider the wider system and its objectives<br>• Does not demonstrate understanding the need for independent assurance<br>• Cannot explain how different approaches to products, implementation and operational assurance can be effective<br>• Cannot demonstrate how they have gained independent assurance in their designs<br>• Focuses on specific aspects of assurance such as certifications rather than determining | • Describe a system where you have designed the security architecture<br>• What made this different to established patterns?<br>• Describe your technical solution [expect good level of technical detail]<br>• How does your solution manage the risks?<br>• Why is this the best way to meet the business need?<br>• What was the outcome of this design?<br>• What are the residual risks and how are they managed?<br>• Describe how you have involved subject matter experts to improve your designs<br>• Pick a few other candidate case studies to assess the candidate's breath of design skills.<br>• Can you provide some examples of assurance activities and explain what the value of these were? | | |

| | | | | |
|---|---|---|---|---|
| | overall confidence at a system level<br>• Cannot articulate detailed technicalities of the architecture<br>• Architectures discussed are fairly standard, with little evidence that they have solved new and challenging problems | • How did you work with the risk appetite to gauge appropriate assurance? | | |

| 4. Thought Leadership – 10 – 15 minutes | | | | |
|---|---|---|---|---|
| **Pass indicators** | **Fail indicators** | **Sample questions** | **Score** | **Comments** |
| • Shows a proactive approach to sharing novel techniques<br>• Publishes guidance within their local community or wider as to how to solve novel architectural challenges<br>• Works to expand the understanding of how to manage risks and design secure architectures with non-security professionals such as developers and vendors<br>• Educates non-technical security professionals such as risk managers in key architectural concepts that contribute to overall system security. At Certified level , this is expected to be more **systemic to a community** than on a 1-1 basis<br>• Contributes findings and techniques to wider communities through mediums such as conferences or training<br>• Has one or more technology specialisms and can demonstrate that they are seen as an expert in secure design by the local community | • Does not share what they have learnt<br>• Works in isolation of the wider technology community<br>• Does not publish guidance or documentation of what they have learnt or developed; keeps knowledge to themselves<br>• Does not take an interest in technology more generally and understand how security can be overlaid on novel technologies<br>• **Just providing leadership within a project or to individuals in their local area** | • Describe when you have shared new techniques or approaches with the community<br>• How did you do this?<br>• What audience did you aim to reach?<br>• How have you tried to improve the understanding of security architecture and risk management in non-security professionals?<br>• Describe when you have worked with non-technical security professionals to increase their ability to understand the risks associated with particular technical approaches and solutions<br>• What would you say your technical specialism is? How have you helped the wider community understand how to overlay security on that technology? | | |

## 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:<br>*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.<br><br>NOTE:<br>Referees' permission to be named must be obtained before being provided.<br>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).
- NCSC Certified Cyber Security Scheme head consultants and NCSC staff members holding a minimum of security architecture skill 6.4 level 3 may vouch for the foundational knowledge of applicants with whom they have worked in the previous 2 years for a period of no less than 12 months.

## Referees

All CVs and case studies must be supported by a referee. The same referee may support more than one role or case study if they can genuinely validate them. 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
- A certificate(s) or other appropriate proof in support of the foundational knowledge requirements above, including, where appropriate, details of the person vouching for a candidate's foundational knowledge to enquiries@ncsc.gov.uk
- A CV of no more than 2 sides of A4 (font size 10) covering the last 5 years of employment and including referees
- A case study (up to two per specialism will be accepted), which describes how you have met all the criteria for the specialism

## 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[27] and will be destroyed within 6 months of the interview in line with

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

Certification Bodies' appeals policies. Certification Bodies are solely responsible for ensuring they comply with all data protection and data storage requirements

## 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.<br>• Suppressing findings that the client representative does not wish to hear.<br>• Recommending inappropriate products or services.<br>• 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.<br>• 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.<br>• 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.<br>• Recommending actions which conflict with NCSC guidance.<br>• Undertaking security testing without client permission. |
| Competence | • Maintaining and updating knowledge and skills and providing evidence of this.<br>• Ensuring advice is proportionate with business objectives and the level of information risk . | • Undertaking work which you know you are not competent to undertake.<br>• Presenting yourself as having a higher level of competence than is actually the case.<br>• Recommending work that is disproportionately large to business requirements.<br>• 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.<br>• 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.