National Cyber
Security Centre
a part of GCHQ

Cyber Security Consultancy Standard

Cyber Security Consultancy Standard
Version 1.3

About this document

NCSC has developed the Cyber Security Consultancy Scheme to certify services provided by consultancies, rather than individual consultants. This document sets out the standard which consultancy services are assessed against.

Related documents

- *NCSC Professional Cyber Services Application Form*
- *NCSC Professional Cyber Services Framework*

Document history

Version	Date	Notes
1.0	2015	Initial release
1.1	2016	Incorporated changes to the professional requirements for Head Consultants leading a risk assessment or risk management service
1.2	2018	Amended to reflect formation of NCSC
1.3	2019	Addition of Ethics record requirement

Contact 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

Section 1 Assessment approach

NCSC has developed the Cyber Security Consultancy Scheme to certify services provided by consultancies, rather than individual consultants. This document sets out the standard which consultancy services are assessed against.

Applications to join the scheme should be made using the *NCSC Professional Cyber Services Application Form*. Applications will be assessed by NCSC using a pass or fail approach. There are two stages to the assessment process:

Stage 1: assessment against the *NCSC Professional Cyber Services Framework*

Stage 2: assessment against the Cyber Security Consultancy Standard (i.e. this document), using:

- evidence submitted in the application
- customer points of contact from case studies
- NCSC-led interview of the Head Consultant(s) and Services Owner(s) (where applicable)
- other evidence NCSC considers relevant (e.g. customer feedback)

The service put forward for certification must pass **both** stages.

Section 2 Requirements

2.1 Service description

The consultancy service offered will be clearly defined and include one (or more) of the categories below:

- Risk Assessment
- Risk Management
- Security Architecture
- Audit & Review

2.1.1 Evidence to be submitted

Companies must identify the categories which the overall consultancy service being assessed includes, and provide a high level description of each. The way in which the consultancy service delivers each selected category must be clearly explained and include a concise description of what is offered.

2.1.2 Notes for applicants

Where services offerings do not align well with categories, a best fit should be identified. The example service offerings presented for each category in the table below are provided for guidance, and are not assessment criteria.

Service offerings may be put forward against one or more categories. A typical category is not expected to include all service offerings. Other services the company may provide will not be covered by this certification.

Table 1 Cyber Security Service Categories

Category	Example service offerings
Risk Assessment	• The provision of advice and guidance to clients to help them understand what approach to risk assessment is right for them in the context of what they are doing and what business outcomes they wish to achieve. • Working with clients to help them develop a realistic view and understanding of the cyber security risks that are associated with their business objectives. • Undertaking and documenting risk assessments on behalf of clients to help them identify and tackle cyber security risks relevant to what they are doing and what they are trying to achieve. • The communication of risk assessment outcomes to clients in ways that support effective security and business decision making.
Risk Management	• The provision of advice, guidance and recommendations on how identified cyber security risks could be managed to help clients make risk decisions and develop strategies for risk management. • The provision of advice and guidance on the effective application of recognised risk management frameworks and/or methods. • The provision of cyber security control recommendations aimed at providing through life management of identified risks. • The development and documentation of risk management plans that are appropriate for the client's business and take into account what they are doing and what they are trying to achieve. • The provision of advice and guidance to help clients develop approaches that ensure the continuous management of identified risks which evolve to cope with changes in, for example the business, threat and technology landscape.

Category	Example service offerings
Security Architecture	• Working to build and or design architectures that manage identified risks, using proportionate controls. • Identification and articulation of risks in the abstract and detailed design of systems and services. Guidance on how to reduce the likelihood of exploitation of vulnerabilities or to constrain impact in the event of a compromise. • Guidance on secure development, build, deployment, operation and management of systems and services. • Guidance on adoption and secure implementation of common architectural blueprints or patterns. • Guidance on selecting technologies which provide adequate mitigation to potential vulnerabilities identified in a system architecture. • Summarising technical security analysis into plain English for different stakeholders.
Audit & Review	• The provision of advice and guidance to clients on how to maintain the relevance of, and ensure the continuous improvement of, internal or external cyber security standards, policies and procedures. • The provision of advice and guidance to clients in support of satisfying or maintaining certification or compliance requirements. • The review of existing cyber security policies and procedures used by clients and the recommendation of changes or improvements. • The review of cyber security artefacts for example, designs, risk analysis, security claims provided by clients or third party business partners, in support of audit activities. • The conduct of checks, reviews and audits and provision of reports to provide client organisations with confidence that internal and external cyber security policies, procedures, and external security requirements are being complied with.

2.2 Consultancy lifecycle

The consultancy service will have an effective lifecycle in place for work delivered. This must cover the full life of each piece of work from ‘offering’, through ‘execution’, and to ‘closure’.

2.2.1 Evidence to be submitted

Companies must describe their standard lifecycle for work delivered by the consultancy service.

2.2.2 Notes for applicants

It is expected that a lifecycle will already be in place, companies are not required to create new processes and documentation. Reference to relevant sections of existing documentation (such as supporting processes and company policies) is encouraged. Referenced material should be made available with the application.

An example of the stages in a lifecycle, and the associated activities which would be described, is given below. Companies are not required to use this (or any other) published standard[1].

The lifecycle should be reflected in the case studies provided in Section 2.5, with an explanation provided for any deviations from the lifecycle.

[1] ISO 20700 provides a useful source of guidance and good practice on consultancy lifecycles

2.2.3 Example lifecycle stages

Offering: activities that take place before the execution of a consultancy assignment:

- pre-sales and identification of client needs
- creation of an agreement, typically covering
  - context of the work
  - services and deliverables
  - approach and work plan
  - roles and responsibilities

Execution: delivery of the services agreed at the offering stage to satisfy the client:

- refining the work plan
- implementing the agreed work plan
- assignment of staff, management and mentoring
- approval and acceptance

Closure: activities that take place at the end of a consultancy assignment:

- final client evaluation and agreement that the service has been delivered
- conclusion of obligations
- finalising payment
- any subsequent improvements to the service

2.3 Consultancy Service Owner

The company must have a defined Service Owner role. This role could be carried out by the Head Consultant, or could be an independent role (possibly with a supporting team) depending on the structure of the company. This role will manage, resource and monitor the consultancy service provided by the company.

The Service Owner is responsible for the following activities:

- fulfilling the company's ongoing obligations
- having overall responsibility for the delivery of work throughout the consultancy lifecycle for the stated service
- acting as the primary contact with NCSC

Each service must have only one defined Service Owner; *accountability* for the service resides with them.

2.3.1 Evidence to be submitted

Companies must provide details of the Service Owner who is responsible for the consultancy service. If more than one Service Owner is to be put forward, their details must also be provided.

Companies must provide a clear definition of the scope and responsibilities of the role, specifically in relation to the consultancy service(s) being offered.

Service Owners may be interviewed by NCSC where a company believes that their attendance may help to clarify a company's service in relation to the overall consultancy lifecycle management. All interviews, including those of the Head Consultant, will seek to verify the role of the Service Owner in a company's consultancy lifecycle and how the role relates to the duties/activities listed below.

2.3.2 Role of the Service Owner

NCSC expects the consultancy Service Owner to have an involvement with the consultancy service they are responsible for. Whilst it may not be possible (and in some cases highly unlikely), that the consultancy Service Owner is involved in all aspects of the execution of the consultancy service, direct accountability and ownership must still reside with them.

The Service Owner's duties/activities will usually include, but are not limited to:

- co-ordination of the consultancy service to ensure related activities are in line with the company's work methodologies and consultancy lifecycle
- advising, with the assistance of appropriately skilled personnel, on applicable methods in support of the delivery of the consultancy service
- monitoring and reviewing the work of the consultants and other team members as appropriate
- developing and managing change control procedures, and making or obtaining necessary decisions for time and cost control
- receiving regular status reports for each consultancy task carried out by the company;
- reporting to the client at regular intervals on progress or, as necessary, requesting further instructions or approval to proceed
- maintaining a relationship with NCSC for the escalation of incidents, issues or risks which may impact the ability of the company to meet its obligations

2.4 Head Consultant

The company must have a Head Consultant who executes the service on their behalf. The Head Consultant must meet and maintain all of the relevant professional requirements for the effective execution of the consultancy service.

The Head Consultant will perform the role identified in Section 2.4.3 and have the competency knowledge and experience necessary to maintain their good professional standing in this role. Each Head Consultant must meet all of the relevant professional requirements listed in Section 2.4.4 .

A service may have more than one Head Consultant, provided they each meet all of the relevant professional requirements listed in Section 2.4.4. In this scenario, a single Head Consultant must still be identified as *responsible* for the execution of each consultancy task.

2.4.1 Evidence to be submitted

Companies must have a Head Consultant who is responsible for the technical execution of the service. If more than one Head Consultant is to be put forward, their details must also be provided.

Each Head Consultant put forward must be supported by evidence that they satisfy the professional requirements.

Head Consultants will be interviewed by NCSC. This interview will seek to verify their competency, knowledge and experience, and - using the case studies provided - explore how they successfully execute their duties and responsibilities in Section 2.4.3 within the consultancy service.

2.4.2 Notes for applicants

The professional requirements will depend on the categories identified as included in the service in Section 2.1. Copies of qualifications/certifications used as part of this application must be submitted with the application. Electronic copies are sufficient.

2.4.3 Role of the Head Consultant

Head Consultants will be actively involved in the consultancy service offering they are responsible for. Whilst the Head Consultant is unlikely to personally deliver all aspects of the service, they are responsible for ensuring that it is delivered to a high standard, and for the overall quality of the technical output of a service offering. Work may be carried out by a team with a range of professional skills and experience.

The Head Consultant's duties / activities will usually include, but are not limited to:

- identifying and fulfilling customer requirements with regard to the consultancy service
- ensuring that individuals assigned to a task have the appropriate technical competency
- maintaining effective communication channels with the customer, the company and the consultancy Service Owner and all other interested parties
- carrying out and supervising work tasks within their area of expertise
- monitoring and reviewing the work of the consultants and other team members as appropriate
- reviewing the progress of design work in conjunction with relevant parties
- reporting to the consultancy Service Owner at regular intervals on progress or, as necessary, applying for further instructions or approval to proceed
- escalating any risks or issues to the consultancy Service Owner as appropriate
- knowledge transfer to other individuals within the company

2.4.4 Professional requirements for the Head Consultant

The professional requirements for the Head Consultant are shown in the table below. Where more than one category is identified as being included in the service, the professional requirements for all categories identified must be satisfied.

Table 2 Professional Requirements for Head Consultants

Category	**Corresponding Core Skill as Part of NCSC Certified Professional (CCP) Role at Senior or Lead**		**Corresponding Professional Certifications**		**Corresponding Academic Qualifications**[2]
Risk Assessment	B1 core skill assessed at Level 3	**OR**	Certified Information Systems Security Professional (CISSP) or Systems Security Certified Practitioner (SSCP) or Certified Information Security Manager (CISM) or Certified in Risk and Information Systems Control (CRISC) or Certified Authorisation Professional (CAP) or Certified Protection Professional (CPP)	**OR**	GCHQ certified Master's degree in cyber security Or PhD that is relevant to the risk discipline and can be applied to cyber security[3]
Risk Management	B2 core skill assessed at Level 3		As above		As above

[2] Individuals who hold the same certified Master's degree in cyber security from an academic institution prior to GCHQ certification may also meet this requirement; this will be assessed on a case by case basis.

[3] These will be assessed on a case by case basis; NCSC may request abstracts or theses to support assessment.

Security Architecture	C1 core skill assessed at Level 3				
Audit & Review	G1 core skill assessed at Level 3		CCP Role at Senior or Lead, and Certified Information Systems Auditor (CISA) or Certified Internal Auditor (CIA) or Qualification in Internal Audit Leadership (QIAL) or Institute of Internal Auditors (IIA) Diploma or IIA Advanced Diploma		

In the future, NCSC may include additional professional certifications and academic qualifications. Please contact NCSC at: certifiedcybersecurity@ncsc.gov.uk to propose alternative professional certifications for consideration. As a guide, proposed professional certifications should:

- be directly applicable to the category
- be vendor neutral
- require an examination
- require evidence of professional practice
- require continued learning, or periodic recertification

Awards which are no longer valid, or associate membership of professional bodies in lieu of professional certifications will not be considered.

2.5 Delivery

The consultancy service will have a track record of high quality delivery, led by Head Consultants using the standard lifecycle.

2.5.1 Evidence to be submitted

The company must provide case studies based on work delivered by the service to clients within the last three years. There must be a sufficient number of case studies to show how each Head Consultant has led work for each category identified in Section 2.1. A case study may cover more than one of the identified categories.

Each case study must:

- demonstrate how the Head Consultant worked with the standard lifecycle to deliver the needs of the client ethically and professionally, making clear their duties/activities
- explain any deviations from the standard lifecycle, including the rationale for following an alternative process, and how governance was maintained
- make clear the way in which the consultancy service provided addresses the category (or categories)
- provide a customer point of contact

2.5.2 Notes for applicants

Feedback received from the customer will be used as part of the assessment. NCSC will need to be able to make contact with the nominated customer point of contact.

Work covered by a case study, and customer point of contact, may be the same as that provided for the Cyber Service Framework assessment.

Case studies will be used to provide context when interviewing the Head Consultant.

2.6 Ongoing obligations

The consultancy service will continue to meet the requirements of this standard set out in sections 2.1 to 2.5. The company will provide sufficient timely and accurate information on the status of, and material changes to, their service to maintain confidence in the service.

The company will also meet the records and reporting requirements described below.

2.6.1 Evidence to be submitted

Companies must confirm that the ongoing obligations, including records requirements and reporting requirements are, and will continue to be met.

2.6.2 Notes for applicants

It is expected that consultancies will already monitor and record the information required as part of running the service.

Failure to provide accurate and timely information may result in NCSC suspending or terminating certification.

2.6.3 Records Requirements

In addition to the requirements in Section 4.II and 4.V of the *Cyber Service Framework Application Form*, companies must provide NCSC with:

1. The record of work in progress/completed by the service, as detailed in Section 4.II of the *Cyber Service Framework Application Form*, every 6 months.
2. A list of all Head Consultants for the service, every 6 months, starting from the date of initial certification, and, detailing for each individual:
    - name
    - CCP role(s)
    - CCP level(s)
    - relevant professional certifications or academic qualifications, as applicable
    - employment status
3. Confirmation that a record is kept which demonstrates that all staff involved in the delivery of the service have seen and agreed to either the NCSC Certified Professional Code of Ethics (in Section III of the CCSC application form) or to at least an equivalent alternative.

2.6.4 Reporting requirements

In addition to the requirements in Section 4 of the Cyber Service Framework Application Form, companies must notify NCSC without delay if:

- the service is no longer able to meet any requirement of this standard
- the status of any certification held by the consultancy (used to secure scheme membership) changes

NCSC requires notification of changes within 1 week if:

- the employment status of the Head Consultant changes
- the Head Consultant no longer meets the relevant professional requirements, (for example due to the lapsing of a professional certification)
- the responsibilities of the Service Owner, including the scope of the role, changes in relation to the execution if the delivery of the consultancy service
- a client (or former client) takes legal proceedings against the service

Notification should be sent by email to certifiedcybersecurity@ncsc.gov.uk or post using the address given on page 1 of the *NCSC Professional Cyber Services Application Form*. Following this NCSC may ask for further information, and/or may then take action e.g. suspending certification.