National Cyber Security Centre
a part of GCHQ

Cyber Resilience Audit Scheme Standard

Version 1.0
July 2024

Document history

Date	Version	Change history details	POC
15/07/2024	1.0	Final Version	CRA Service Management Team

A review will take place October – December of each year for publication the following February.

Document owner

National Cyber Security Centre (NCSC). All material is UK Crown Copyright ©

Abbreviations/Definitions

Agreement	Means the Ecosystem Agreement between the NCSC and the Company, including all Schedules, as amended from time to time.
Company (and "Companies" shall be interpreted accordingly)	Means the company which is, or is applying to become, a Scheme member.
CRA	Means a cyber resilience audit, an independent audit carried out against a cyber security standard, such as the CAF.
CRA Scheme Standard	Means the standards which must be met to be part of the Scheme. Referred to as the Standard.
CRA Team	Means the team of individuals carrying out a CRA on a Customer's scope.
CRA Head Consultant	Means the person in the Company responsible for the technical delivery of the CRA service.
CRA Service Owner (SO)	Means the person in the Company with overall responsibility for the CRA service.
CRA Team Leader	Means the NCSC-approved Company staff member appointed to lead teams during a CRA.
Customer	Means the organisation which contracts with the Company for a CRA.
Cyber Assessment Framework or CAF	Means the tool created by the NCSC for assessing how well operators of essential

	services are managing cyber security risks under the NIS Directive.
Cyber Oversight Body	Means an entity responsible for understanding the extent to which all the organisations in a sector are successfully managing cyber risks, such as a cyber regulator or a government policy organisation.
NCSC	Means the National Cyber Security Centre.
Scheme	Means the NCSC's CRA scheme.
Scheme Partner	Means a Cyber Oversight Body that chooses to use the Scheme in their sector.
We/Us/Our	Means the NCSC.
You/Your	The Company which is, or is applying to become, a CRA Scheme member.

Scheme Membership Requirements

1. This document defines the standards required for membership of the Cyber Resilience Audit (CRA) Scheme. You must read this Standard in conjunction with the Scheme's Working Practices Document and the Ecosystem Agreement. You must always (unless otherwise approved by the NCSC):

    - satisfy all the requirements defined in this Standard
    - meet the requirements of the overarching Ecosystem Agreement
    - work in accordance with the Scheme Working Practices Document
    - be regularly performing CRAs.

The Company Standard

Network Security

2. You must maintain an in-date Cyber Essentials Plus certification for all the systems on which information related to Customers' engagements is stored and processed.

Personnel

3. You must conduct all of the following activities. We have divided them into three categories and given a role title to each. These role titles may not exist in your Company, but we do expect there to be a defined person who is accountable to the NCSC for ensuring they are conducted.

4. The same individual may fulfil more than one of these roles:

   - Business requirements – "CRA Service Owner".
   - Technical Health of the CRA service – "CRA Head Consultant".
   - Technical Oversight of individual CRAs - "CRA Team Leader".

CRA Service Owner (SO)

5. While we do not expect one individual to personally deliver all aspects of the CRA service, the named CRA Service Owner must be directly accountable for delivery of the Service. Under the Scheme, the following tasks are all mandatory:

   a. Acting as the NCSC's primary contact for all Scheme communications and all onward action.

   b. Positively contributing to the wider CRA Scheme community. This includes:

- contributing to CRA Scheme improvements;
- taking an active part in community meetings
- meeting with the NCSC from time to time, as requested.

c. Actively ensuring that the Company meets all its obligations under this Standard and the associated Agreement.

d. Submitting, on time or when requested, an annual Management Information Report to the NCSC (a template will be provided), including in accordance with the terms of the Agreement.

e. Documenting and maintaining Company quality management processes as they apply to the CRA Scheme.

f. Reviewing and updating Company processes in accordance with the CRA Scheme Standard.

g. Ensuring that everyone involved in the provision of the CRA service adheres to the Company's own documented processes.

h. Providing the Company's Cyber Essentials Plus certificate number to the NCSC on an annual basis.

i. Maintaining accurate Company records and providing these to the NCSC when requested, including in accordance with the terms of the Agreement.

j. Actively monitoring and managing Customer relationships and seeking feedback to provide evidence of satisfaction with the Company's work, in accordance with the terms of the Agreement.

CRA Head Consultant

6. The named CRA Head Consultant must hold a UK Cyber Security Council Professional Registration for the Cyber Security Audit & Assurance specialism Chartership Title. More information about the UK Cyber Security Council Professional Registration, (available here).

7. The CRA Head Consultant must be directly accountable for the technical health of the CRA service, which includes the following mandatory tasks:

   a. Acting as the NCSC's primary contact for all technical feedback and questions regarding the technical aspects of the CRA service, and any onward action required.

   b. Defining, implementing and maintaining an appropriate audit methodology, which is clear to the Customer and takes account of their requirements.

   c. Conducting reviews of audit quality management processes and documentation on a regular basis and when directed by the CRA Service Owner.

   d. Ensuring the technical quality and standard of delivery of the CRA service and maintaining the overall technical health of the CRA Team.

   e. Accountability for the quality of reports, ensuring they meet both the Company's own standards, and Scheme Partner direction and requirements (where applicable). We do not expect the CRA Head Consultant to personally quality control every report, but we do expect the Company to have and adhere to a quality control process, for which the CRA Head Consultant is accountable.

   f. Ensuring all CRA Team Leaders have appropriate professional training and development plans. This may include:

      - Identifying mentors for inexperienced CRA Team Leaders.

- Ensuring there is a training lead for CRA Team Leaders.

g. Being responsible for identifying the skills and personnel needed to meet the Customer's or, if applicable, Scheme Partner's scope and requirements. This includes ensuring that everyone involved in delivering a CRA has read and understands the latest version of the CAF and all associated documentation, (available here).

h. Attending the NCSC CRA Scheme training and any sector-specific training.

CRA Team Leader

8. A CRA Team Leader must hold a minimum of UK Cyber Security Council Professional Registration for the Cyber Security Audit & Assurance specialism Principal Title. More information about the UK Cyber Security Council Professional Registration, (available here).

9. The CRA Team Leader must be responsible for the delivery of a specific Customer engagement. This includes the following mandatory tasks:

   a. Must be contactable by all members of the CRA Team and by the Customer for the duration of the engagement.

   b. Is responsible for the behaviours, actions and advice given by their CRA Team.

   c. Is responsible for conducting the CRA in accordance with Scheme Partner's publications or guidance, where they are applicable.