National Cyber Security Centre
a part of GCHQ

Cyber Resilience Test Facilities

Scheme Standard

Version 2.0

Oct 2026

Document History

Date	Version	Change history details	POC	SharePoint Ref
21/05/2025	1.0	Final Version	Technology Assurance Management Team	NCSC-1015903574-1728
14/10/2025	1.1	• Removal of the Implementation Guidance (formerly Section B) as not required within the standard. • Changes to reflect that the *Product Assessment Report (PAR)* template will be issued directly to CRTFs. • Minor updates to improve clarity.	Technology Assurance Management Team	NCSC-1015903574-1748
29/10/2026	2.0	• Inclusion of Sanitisation Service Assurance as an additional CRTF Service offering. • Recommendations from the UKAS Scheme review implemented to improve clarity.	Technology Assurance Management Team	HV4NKQ6VV52Y-1968710376-30055

A review will take place annually (October – December) of each year for publication the following January/February.

Document owner

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

Contents

ABBREVIATIONS/DEFINITIONS 6

INTRODUCTION 7

About Cyber Resilience Test Facilities Scheme 7

Approval 8

CRTF Scheme Annual Review 8

Communicating Changes in the Scheme Documentation 9

Transitional Arrangements Between Versions of the CRTF Scheme Documentation 10

Fraudulent Evaluation Claims 10

Point of Contact 10

SECTION 1 – CRTF SET-UP AND ONBOARDING REQUIREMENTS. 12

CRTF General Requirements 12

Impartiality 12

Management Objectives 12

Common Competence Requirements 13

Outsourcing Assessment Activities 13

Quality Management 13

Security 14

Evaluation Facilities 15

Certification, Accreditation and Training Requirements 16

Essential Skills 16

Useful Skills 17

SECTION 2 - TRIAL EVALUATION 18

Purpose 18

Objectives 18

Product or Service Selection 18

Assessment Process 19

Completion 19

SECTION 3 – ASSESSMENT REPORTING GUIDANCE 21

Summary 21

Introduction 21

Definition of Terms Used in Output Documents 21

Format of the Full Report 22

Format of the Assessment Report 23

ANNEX A – CYBER RESILIENCE TESTING (CRT) 24

INTRODUCTION TO CRT 24

CRT EVALUATION PROCESS 24

Summary 24

Preparation 25

Planning 25

Analysis 25

Report Writing and Completion 25

ADDITIONAL SET-UP AND ONBOARDING REQUIREMENTS 26

Requirements to Deliver CRT Assessments 26

Trial Evaluation 26

Product Assessment Reporting 27

ANNEX B - SANITISATION SERVICE ASSURANCE 28

INTRODUCTION TO SANITISATION 28

Summary of Service Requirements 29

Location of Sanitisation Activities 29

Health and Safety 29

SANITISATION EVALUATION PROCESS. 30

Summary 30

Preparation 30

Planning 31

Analysis 31

Report Writing and Completion 31

Ongoing Maintenance of the Sanitisation Services 32

ADDITIONAL SET-UP AND ONBOARDING REQUIREMENTS 33

Requirements to Deliver Sanitisation Assessments 33

Trial Evaluation 33

Sanitisation Assessment Reporting 34

Abbreviations/Definitions

Agreement	The “assurance ecosystem agreement” entered into between the NCSC and the Company, including all Schedules, as amended from time to time.
APC	Assurance Principles and Claims.
CAE	Claims, Argument, Evidence.
Client	The end user or buyer of a product or service.
Company (and “Companies” shall be interpreted accordingly)	The company which is, or is applying to become, a CRTF.
Customer	Means the organisation which contracts with the Company for the provision of CRTF Services.
CRT	Cyber Resilience Testing.
CRT APC	The Cyber Resilience Testing (CRT) Assurance Principles and Claims (APC) means the standard against which products are assessed for the CRT service offering.
CRTF	Cyber Resilience Test Facility.
CRTF Lead Evaluator	The individual with overall responsibility at the Company carrying out the CRTF Services.
CRTF Team	The team of individuals at the Company carrying out the CRTF Services.
Evaluation	The process of gathering and assessing the evidence provided in support of the Assurance Principles and Claims to produce the required output reports.
NCSC	The National Cyber Security Centre.
ESM	Electronic Storage Media.
PBA	Principles Based Assurance.
Product	The connected item that is the subject of the evaluation.
Assessment Report	The evaluation output report that shall be made available by the customer to the end user or buyer of a product or service.
Sanitisation APC	The Sanitisation Assurance Principles and Claims (APC) means the standard against which the Service is evaluated for the Sanitisation Service offering.
Scheme	The Cyber Resilient Test Facilities Scheme.
Scheme Standard	The standards which shall be met to be part of the Scheme as set out in this document.
Scheme Documentation	All documents issued for the management and delivery of the CRTF Scheme and includes: the CRTF Standard, APCs, Assessment Report Templates, Applications Forms and all such other documents that may be issued from time to time.
Service	The service that is the subject of the evaluation.
Service Provider	The company that delivers the assured service to the Client.
We/Us/Our	The NCSC.
Vendor	The Developer, Manufacturer or Reseller of the Product under evaluation.

Introduction

About Cyber Resilience Test Facilities Scheme

1. The NCSC has developed a new UK assurance methodology to enable vendors and service providers to demonstrate the cyber resilience of their connected products or assurance services in a structured and consistent way.

2. CRTFs will deliver this new assurance methodology for a wide range of connected products and services using the Principles-Based Assurance (PBA) methodology, as part of a wider NCSC transition away from compliance-based assurance schemes as described in The future of NCSC Technology Assurance White Paper. This will enable consumers of technology to have confidence in the cyber resilience of the connected products and services they purchase whilst at the same time extending the reach of NCSC by harnessing industry to deliver assurance for a much wider range of cyber products and services than is possible today.

3. The CRTF scheme objectives are to:

   a. Create a national ecosystem of assured test facilities to provide buyers with confidence in the cyber resilience of the connected products and services they purchase.

   b. Boost confidence in the technology supply chain through enabling better decision-making.

   c. Enhance the wider UK resilience to cyber threats through the development of deeper understanding of cyber risks.

   d. Promote best practice amongst technology vendors and service providers by encouraging further engagement and understanding of cyber risk across the market.

4. This document details the standards and onboarding requirements that apply to a Company becoming a NCSC assured service provider, subsequently referred to as a Cyber Resilience Test Facility (CRTF). It also lays out the additional requirements for each service offering than can be delivered by CRTFs.

5. In accordance with the details in Annex F of the Agreement CRTFs may be authorised to deliver one or more of the following services:

   a. Annex A - Cyber Resilience Testing (CRT).

   b. Annex B - Sanitisation Service Assurance.

6. All CRTFs are onboarded as capable and competent in the delivery of the initial service offering that assesses connected products against the Cyber Resilience Testing (CRT) Assurance Principles and Claims (APC)[1] which has been aligned with the Software Security Code of Practice.

Approval

7. Approval to operate as a CRTF is subject to the terms and conditions in the Agreement between NCSC and the Company. Approval will only be confirmed when both the Company and NCSC have signed the Assurance Ecosystem Agreement for the CRTF scheme following accreditation against ISO/IEC 17020.

8. NCSC approval to operate as a CRTF does not imply any guarantee of business.

9. Details of approved CRTFs and the services which they are approved to deliver will be published on the NCSC website.

CRTF Scheme Annual Review

10. The CRTF Scheme will be reviewed on an annual basis between October and December with updates being published the following February as required. Information to support the review will be gathered throughout the year from stakeholders and interested parties primarily through the following mechanisms:

a. The CRTF Community of Interest Forum – Designed to continuously review and improve the operation of the scheme through updates to Scheme Documentation, monitoring of standards and introduction of new services. It will be held every 6 months (in May and November) with representations from the CRTFs, NCSC Scheme management and key stakeholders from Government and Industry as appropriate to the specific focus of each event.

b. The CRTF Scheme Management Information Report submitted annually by all CRTFs in accordance with Schedule 5 of the Agreement.

c. UKAS feedback on the CRTF ISO/IEC 17020 accreditation process.

d. Feedback through the CRTF Service Monitoring and Improvement Plan.

[1] The CRT APC can be downloaded from the NCSC website here - Assurance Principles and Claims documents - NCSC.GOV.UK

e. Feedback from vendors, service providers and customers gathered through NCSC wider sector engagement, conferences, working groups and meetings.

f. Direct feedback via the ncscindustryassurance@ncsc.gov.uk mailbox.

11. The CRTF Scheme annual review will as a minimum consider the following aspects:

a. Updates to Scheme Documentation, training and the delivery of new and improved service offerings.

b. Assessment standards and consistency of reporting.

c. Requests for clarification related to scheme requirements.

d. Feedback from stakeholders and other interested parties.

e. Responsiveness of scheme owners to requests of information.

f. The need for validation audit or other checks as required to review scheme memberships in accordance with Section 3.3 of the Agreement.

g. Whether the scheme is fulfilling its objectives.

h. Whether the scheme is operated by competent, consistent and impartial inspection bodies.

i. Whether the scheme requirements are being applied in a consistent manner.

Communicating Changes in the Scheme Documentation

12. When changes to the Scheme Documentation are introduced, the following measures will be taken to inform all users and interested parties:

a. Notification of upcoming changes to Scheme Documentation will be promulgated in advance through the CRTF Community of Interest Forum, such notifications will include details of the nature and extent of the change and the expected timeframe for implementation.

b. On the publication of the updated Scheme Documentation:

i. All registered CRTFs and UKAS will be notified by CRTF Scheme Manager. Such notifications will include confirmation of the details required for implementation.

ii. The NCSC CRTF website pages will be updated to reflect the changes and include details required for implementation.

Transitional Arrangements Between Versions of the CRTF Scheme Documentation

13. When changes to the CRTF Scheme Documentation are implemented, the following factors will be considered in determining the transitional arrangements and timeframe for implementation:

a. The extent and nature of the changes to determine the requirement for any further assessment activities by the Authority or UKAS.

b. The extent and nature of the changes to determine the requirement for any CRTF revaluation activities in relation to previously issued *Assessment Reports*.

c. Consultation with UKAS to determine the timeframe required for any additional assessment activity needs to be undertaken.

d. A deadline for implementation will be agreed in consultation with UKAS and the CRTF CoI Forum.

Fraudulent Evaluation Claims

14. The CRTF shall notify the NCSC immediately upon becoming aware of any fraudulent, misleading, or unauthorised claim relating to its evaluation activities under the scheme, to enable appropriate action to be taken and to help safeguard the integrity of the scheme.

Point of Contact

15. The NCSC will appoint a Point of Contact for the Company. The PoC will have a thorough understanding of the CRTF service offerings and be able to discuss any problems that may arise. As far as possible, NCSC will endeavour to ensure that the same PoC is responsible throughout the onboarding process from a Company's initial application through to appointment as a CRTF and thereafter for working with the Company during the early years of its membership of the CRTF Scheme.

16. NCSC will also be available to provide support and direction during the Trial Evaluation.

17. Each CRTF shall appoint an individual with appropriate authority to act as point of contact with the NCSC.

18. All day-to-day enquiries regarding the scheme should be made to ncscindustryassurance@ncsc.gov.uk[2].

[2] Add “CRTF” to the beginning of the subject line.

Section 1 – CRTF set-up and onboarding requirements.

CRTF General Requirements

1.1. The Company shall submit the CRTF application form[3] and be accepted by the NCSC as a candidate for CRTF certification.

1.2. The Company shall meet the specific certification, accreditation and training requirements listed in paragraph 1.25.

1.3. The Company shall have the necessary cyber security skills, knowledge and expertise to gather and analyse the evidence required to complete the assurance process. The essential skills required are listed in paragraph 1.27.

1.4. The CRTF Team members undertaking PBA analysis during an assessment shall have completed the Performing Cyber Resilience Testing (PBA)[4] training course to gain the understanding and knowledge required to apply the PBA methodology in the delivery of assurance services.

1.5. The Company shall complete a Trial Evaluation (see Section 2) in order to provide the evidence necessary for UKAS ISO/IEC 17020 accreditation and to demonstrate their ability to conduct a full PBA assessment including the production of the required output reports (see Section 3).

Impartiality

1.6. The CRTF shall be responsible for the impartiality of its evaluation activities and be able to demonstrate those activities are undertaken impartially such that commercial, financial or other pressures that might compromise its impartiality are managed.

1.7. In instances where a threat to its impartiality is identified, the CRTF shall ensure the effect is eliminated or minimised to safeguard impartiality of the evaluation activities.

Management Objectives

[3] The CRTF Application Form can be requested from ncscindustryassurance@ncsc.gov.uk. Add “CRTF” to the beginning of the subject line.

[4] Contact ncscindustryassurance@ncsc.gov.uk for *Performing Cyber Resilience Testing (PBA)* course details and scheduling. Add “CRTF” to the beginning of the subject line.

1.8. The Company shall maintain an effective management system such that the organisational structure of a CRTF provides for a sufficiently high standard of quality in all aspects of its work. This shall be reflected in the quality management system (QMS) and security procedures, which cover all management, security and technical aspects related to assurance process, including the ongoing technical competence of the evaluation team.

Common Competence Requirements

1.9. The CRTF shall have access to competent persons, who have completed the Performing Cyber Resilience Testing (PBA) training course, to perform the type, range and volume of its evaluation activities. It shall ensure that each person clearly understands their duties, responsibilities, and authorities within the scope of the functions they perform.

1.10. The CRTF shall manage the competence of its personnel involved in evaluation activities and shall determine the competence requirements for the evaluation activities/functions performed.

1.11. The personnel performing the CRTF evaluations shall have suitable and sufficient knowledge, to the extent required for their role(s), of the technologies or services being evaluated and the manner in which the cyber resilience can be undermined.

Outsourcing Assessment Activities[5]

1.12. The CRTF shall itself normally perform the evaluation activities that it contracts to undertake. The use of externally provided evaluation activities for part of the CRTF evaluation or the entire evaluation shall only be used in exceptional circumstances (e.g. unforeseen resource constraints or key facilities or equipment becoming unavailable) and only provided by another NCSC recognised CRTF. The CRTF shall inform the vendor of its intention to outsource evaluation activities (in part or in full), to provide the vendor with an opportunity to object in advance. This does not preclude the use of specialist testing organisations to provide evidence, as there are no restrictions on subcontracting evaluation activities to gather evidence against an APC as it's the CRTFs responsibility to assess all evidence and determine whether there are any associated risks to be reported.

Quality Management

[5] Meaning subcontracting to another organisation to provide part of the CRTF inspection activities on behalf of a CRTF.

1.13. The CRTF shall have its own quality management system (QMS) which meets the requirements of ISO/IEC 17020.

1.14. The NCSC reserves the right to review the QMS once per year as per the Agreement.

1.15. The QMS shall ensure that evaluation evidence, together with problems, difficulties, concerns, issues and decisions, is captured, recorded and reported, and appropriately archived[6].

1.16. The QMS shall ensure that information management procedures are adequate to protect the deliverables received from customers, as well as any reports relating to an evaluation.

1.17. The QMS shall ensure that procedures are in place to address general operational topics, including, but not limited to:

a. Disputes and complaints.

b. Use of contractors and subcontractors.

c. Training and technical competence.

d. Handling of evaluation evidence.

1.18. Notwithstanding the requirements of clause 4.5 in the Agreement the CRTF shall have a documented process in place to address any disputes arising from the evaluation decisions and recommendations contained within an *Assessment Report* and resolve legitimate grievances promptly with the customer.

1.19. CRTFs should, on completion of the assurance activities, perform a technical and quality review of their team's work to ensure it is of sufficient quality, that all aspects of the assurance activities have been adequately analysed, and reported, and that sufficient evidence has been gathered for all elements of the assurance activities.

Security

1.20. The CRTF shall have security procedures that set out the procedures and responsibilities to be undertaken by all the CRTF staff, to maintain the confidentiality of all commercially sensitive evaluation information in whatever form.

[6] See Section 7 (Record keeping and review) of the Agreement

1.21. The Company shall have a nominated person responsible for policies and procedures to appropriately manage data. This shall be in accordance with applicable data protection laws that include (but are not limited to) the General Data Protection Regulation (Regulation (EU) 2016/679), the Data Protection Act 2018, and all applicable law about the processing of personal data and privacy. Further details in relation to which are set out in the Agreement.

1.22. In addition, it is recommended that procedures are in place that include (but are not limited to):

a. Physical Security including access control.

b. Personnel Security including Identifying and authenticating staff and visitors.

c. Periodic audit of the procedures.

d. Dealing with security violations.

e. The physical, personnel and procedural aspects of remote or virtual working.

f. Confidentiality and integrity measures to protect sensitive information during all stages of the evaluation away from the CRTF premises, including transmission of evaluation data back to the CRTF.

Evaluation Facilities

1.23. The Company shall be in an appropriately secure area of the company's premises and where appropriate should include the following:

a. Lockable office furniture suitable for storing evaluation resources (supporting documentation, Claims evidence, test results, test reports, etc).

b. Commercially sensitive material shall not be left unsecured out of working hours.

c. Physical access controls that permit access to the CRTF only to authorised staff.

d. Logical access controls that permit access to IT facilities only to authorised users. Accounts shall be unique to individual users, who will be granted only the permissions required for the job. User actions shall be auditable and attributable. Document and record management should support multiple evaluations while maintaining task separation and protecting customer confidentiality.

1.24. Company staff shall be made aware of the commercial sensitivities of the information required for an evaluation and agree to handle this information with due respect and in accordance with the requirements of the Customer.

Certification, Accreditation and Training Requirements

1.25. To deliver technology assurance services under the CRTF Scheme, the candidate Company shall have:

a. A valid Cyber Essentials+ certificate issued within one year before the date of application.

b. A lead assessor in the team certified as an ISO/IEC 27001 Lead Auditor or CISA (Certified Information Systems Auditor).

c. A CISSP (Certified Information Systems Security Professional) qualified member of the team.

d. Completed the approved CRTF training course [7].

e. Successfully completed a Trial Evaluation (to be assessed by NCSC) to demonstrate their ability to apply the PBA methodology for the requisite CRTF service offering and gather information to support ISO/IEC 17020 accreditation.

f. Accreditation to ISO/IEC 17020 “Requirements for the operation of various types of bodies performing inspection” [8].

1.26. Once accredited, a CRTF shall meet its ISO/IEC 17020 obligations, with assessment activities carried out as required by UKAS.

Essential Skills

1.27. CRTFs require a broad range of skills and knowledge in sufficient depth to conduct cyber assessment and assurance activities. These are to be demonstrated through a written submission listing qualifications and experience as part of the application process prior to performing a Trial Evaluation. The essential skills required within the CRTF team are as follow:

---

[7] Contact ncscindustryassurance@ncsc.gov.uk for *Performing Cyber Resilience Testing (PBA)* course details. Add “CRTF” to the beginning of the subject line.

[8] The latest version of ISO/IEC 17020 should be used and is available from ISO - International Organisation for Standardisation.

a. A good understanding of cybersecurity auditing and assurance practice.

b. A good understanding of cyber security risk management, assessment and mitigation.

c. Knowledge of cybersecurity product and/or secure product development processes.

d. Knowledge of cybersecurity product and/or secure product testing.

e. Knowledge of security engineering principles and application.

f. An understanding of the cyber security threat landscape and secure functionality design.

g. An understanding of security operations and incident management.

h. An understanding of the legal and regulatory framework pertaining to cybersecurity.

i. Critical thinking and judgement.

Useful Skills

1.28. In addition to the essential skills, whilst not assessed, it is recommended that the CRTF team should have or gain the following useful skills:

a. Prior knowledge of cybersecurity product and/or secure product evaluation processes.

b. Prior knowledge of the PBA method and application of the CAE[9] approach and APCs.

c. Project management and planning.

d. Report writing and communication skills.

[9] Further details can be found here - CAE FRAMEWORK.

Section 2 - Trial Evaluation

Purpose

2.1. The purpose of the Trial Evaluation is to provide evidence to the Accreditation Body (UKAS), that the Company complies with ISO/IEC 17020 and demonstrate their ability to conduct a full PBA assessment including the production of the required output reports. It is also one of the pre-requisites for approval to operate as an NCSC CRTF.

2.2. A successful trial evaluation is required to be undertaken for each CRTF service offering that the Company intends to offer.

Objectives

2.3. The objectives of the Trial Evaluation are to demonstrate that the:

a. Individual evaluators are technically competent.

b. Management and administration of the Company is competent to fulfil its role.

c. Company can conduct a full PBA assessment against the applicable APC document for the CRTF service being offered.

d. Company can produce the required evaluation output reports.

e. Evaluation reports meet ISO/IEC 17020 and the requirements of the CRTF Standard document.

Product or Service Selection

2.4. The following criteria should be considered when selecting a product or service for the trial evaluation:

a. The Company shall have support from a vendor or service provider and have a product or service to evaluate.

b. The Company shall choose a product or service that can be evaluated against the relevant APC to sufficiently demonstrate the application of the assurance process and produce the information required for UKAS accreditation.

c. The NCSC will need to approve the product or service selected for evaluation and confirm that the Company is suitable to proceed to a Trial evaluation.

d. The Company shall ensure that the vendor or service provider is clear that it is a trial evaluation and additional support may be required. However, if the Company is successful at the end of the trial evaluation, the vendor or service provider will be issued with an *Assessment Report* for the relevant service offering.

e. The Company shall abide by the impartially requirements (see Section 1).

Assessment Process

2.5. At agreed stages during the Trial Evaluation the NCSC will confirm that processes are in place to:

a. Ensure that the vendor or service operator adequately understands the relevant assessment process.

b. Ensure that the Company has sufficient knowledge of the product or service under evaluation.

c. Modify Claims in accordance with the PBA process.

d. Demonstrate that there are effective processes for gathering, collating and analysing the evidence.

e. Assess whether the evidence meets the Claims.

f. Agree and finalise the assurance output reports.

g. Issue the report and manage records.

h. Conduct the evaluation in an efficient manner, so time and financial costs are necessary and proportionate.

Completion

2.6. Upon completion of the Trial Evaluation:

a. The NCSC will provide a written statement of completion that can be used to support ISO/IEC 17020 accreditation against the CRTF *Scheme Standard* via email or other method.

b. And on notification that ISO/IEC 17020 accreditation has been achieved the Company will be awarded NCSC assured service provider status and the authority to

operate as a CRTF in accordance with the assurance services listed in Annex F of the Agreement.

c. The Company shall continue to meet the general requirements listed in the main body of this document and any additional requirements issued by the NCSC as required.

Section 3 – Assessment Reporting Guidance

Summary

3.1. This section provides guidance on the expected structure, contents and purpose of the assurance outputs from Cyber Resilience Test Facilities (CRTFs).

Introduction

Document 1: Full report

3.2. This document is a deliverable to the product manufacturer or service provider from the CTRF as part of their contractual arrangement. Its purpose is to provide the customer with a complete set of findings to enable them to make improvements to their product or service, or plan for future updates of their product or service.

3.3. As this document is designed to only to be released to the customer there is significant leeway for the CRTF and customer to agree on its structure and contents.

Document 2: Assessment Report [10]

3.4. This document is intended for wider release (by the customer) to users/procurers of the product or service and has a more defined format than the full report. This document will typically be more concise than the full report and focus on the actionable information about the product or service that a user should be aware of. This will include significant risks identified and key assumptions supporting the deployment and usage of the product or service. If the Customer wishes to advertise that their Product or Service has been assessed under the CRTF Scheme the *Assessment Report* must be made available in its entirety to an end user or buyer of a product or service on request.

Definition of Terms Used in Output Documents

Assumption

3.5. An assumption is a claim, side-claim or argument that is knowingly not evidenced. There are 3 main types of assumptions:

a. A claim that is out of scope of the assessment. In most cases this will be an assumption that the product or service is deployed or used in a certain way.

[10] CRTF *Assessment Report* templates will be issued separately for each CRTF service that is offered.

b. A claim that is not evidenced as it is as assumed it is not relevant to the products' or services' intended application.

c. A claim that is not evidenced because a design decision has knowingly assumed that any resulting risk will be readily accepted by users.

Doubt

3.6. A doubt is a claim that is evidenced but has failed to demonstrate all aspects of the claim. This is primarily about aspects of a claim that are not evidenced rather than whether evidence offered was considered sufficiently convincing.

3.7. A claim for which there are no Doubts will be called fully met. Again, this primarily means all aspects of the claim have been evidenced, rather than a comment on whether the evidence was sufficiently convincing.

Unmet Claim

3.8. An unmet claim is a claim that evidence has demonstrated to be not met. This may be an unusual event, but could possibly arise as a result of a misunderstanding by a manufacturer of something they have implemented

Modified Claim

3.9. A claim from the APC that has been modified/replaced using an agreed argument linking it to a higher level claim. These Claims are likely to occur where a customer has taken an innovative, or simply different, approach to that suggested or envisage by the APC. Modified Claims are not to be seen in a negative way and are indeed encouraged to allow the APC to be as widely applicable as possible.

Format of the Full Report

3.10. As stated above there is flexibility for the CRTF and customer to agree the format of this report. As such this proposed format is a suggestion only and need not be precisely followed.

3.11. This report will mainly comment at the detailed Claims level, as this information is most likely to be useful to the manufacturer. A simple format could be:

- *Introduction*

- *Findings*

A very brief summary of the Claims that have been fully met. This could be as a little as a list but could include any specific observations the CRTF wishes to make on the

nature or strength of evidence (eg, this was 'really clear evidence', or 'this has been deemed to be fully met, but the evidence was very difficult to interpret').

A tabular presentation of all Assumptions made. These should be linked to the specific claim that the assumption is directly relevant to. The table should also include any relevant comment by the CRTF on the legitimacy of the assumption, and whether the assumption is also reported in the Assurance statement.

A tabular presentation of all the Doubts and Unmet Claims raised. These should be linked to the specific claim they relate to and provide a description of what aspect of the claim the CRTF has considered to be un-evidenced or countered.

- *Conclusions*

Format of the Assessment Report

3.12. The *Assessment Report* is intended for those responsible for making security risk decisions in relation to the procurement, installation, maintenance, or operational use of a product or service. As such it is not assumed that the reader will have read the APC or have any familiarity with the detailed PBA methodology or the terminology of the wider CAE approach.

3.13. The report is aligned with the NCSC risk management guidance:

"Risk Management often requires a relationship between people who analyse risks and the people who make decisions based on that analysis. Communication between these two groups must be clear, understandable and useful. If the people who make decisions can't interpret the analysis they're presented with, then there is little point in doing risk analysis at all."

3.14. It is assumed that the reader understands that the process is assessing a product or service against the pre-defined set of Principles contained in the relevant APC for the Product or Service.

3.15. With these observations in mind the *Assessment Report* will report at the Principle level rather than the detailed Claims level. If required, the latest standard report templates can be requested from the ncscindustryassurance@ncsc.gov.uk[11] team.

[11] Add "CRTF" to the beginning of the subject line.

Annex A – Cyber Resilience Testing (CRT)

Introduction to CRT

A1. Cyber Resilience Testing, known as CRT, is a service that assesses the confidence that a connected product can protect itself when faced with malicious activity from public domains, such as cyberattacks.

A2. CRT uses the Principles Based Assurance (PBA) methodology, providing for flexible and continuous assurance. It allows vendors to demonstrate how well their product satisfies the key principles of good engineering practice and is fully aligned with DSIT's Software Security Code of Practice.

A3. This is achieved through assurance of the quality of the design, build, and ongoing support of the product throughout its lifetime.

A4. CRT does not seek to assess how well a product performs it's intended security functionality, this can be assessed using other assurance services designed for these purposes and will require assessment against additional APCs for the intended functionality.

A5. The *Assessment Report* documents any potential risks associated with the product. This enables customers to make informed decisions, to differentiate between products and supports their appropriate use.

CRT Evaluation Process

Summary

A6. The evaluation process used by the CRTFs should comprise of the following generic stages.

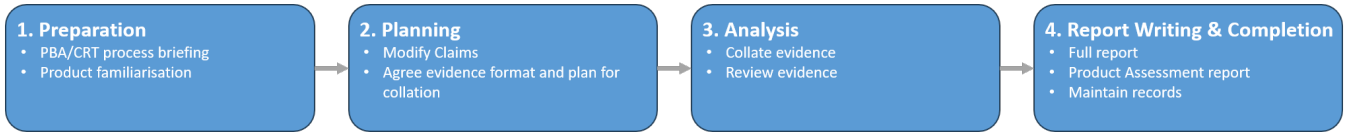


Figure A-1 – CRT evaluation process.

A7. The CRTF Team performing the evaluation may have different roles. There shall be a lead who will be the primary point of contact with the Customer and will be responsible for the overall integrity of the evaluation. An experienced evaluator with knowledge of the specific service offering may perform most of the work.

Preparation

A8. The preparation phase shall ensure that:

a. All evaluations are conducted and owned by a certified ISO/IEC 27001 auditor or CISA (Certified Information Systems Auditor).

b. That the Customer has sufficient understanding of the evaluation and assessment process to complete the evaluation.

c. The CRTF has sufficient understanding of the product functionality to conduct the evaluation.

Planning

A9. During the planning phase the CRTF shall:

a. Agree the Claims to be evidenced and where modifying Claims, ensure it is necessary, appropriate and supported by an appropriate PBA style argument.

b. Agree evidence requirements for each Claim and identify gaps.

c. Create a plan for gathering evidence in the most appropriate manner. No single approach is likely to satisfy every situation.

d. Use effective tools to collate, manage, and share evidence.

Analysis

A10. During the analysis phase the CRTF shall:

a. Develop and use a consistent and repeatable approach to the process of collating and reviewing evidence.

b. Identify and categorise gaps in evidence as risks in accordance with the PBA methodology.

A11. The CRTF Team shall perform evaluation activities sufficient to have confidence that each Principle has been examined and reported on where appropriate.

Report Writing and Completion

A12. Prior to the completion of an evaluation the:

a. CRTF and Customer are required to agree the format of the Full Report that will be issued only to the Customer. The report should enable the Customer to easily identify areas where the development processes, product or working practices could be improved.

b. CRTF will ensure that the *Product Assessment Report (PAR)* [12] adheres to the standard template provided.

c. CRTF is to advise the Customer that making the PAR available to the end user or buyer of a product is a condition of the CRTF scheme [13].

d. CRTF will ensure that evaluation records are updated and maintained as required.

A13. On completion of a CRTF evaluation product vendors may use the following statement for use in their marketing and promotional materials:

NCSC CRTF – Cyber Resilience Assessed

Small print: Assessment conducted via an NCSC Cyber Resilience Test Facility (CTRF) does not imply compliance with regulatory standards, best practice, or any other form of certification.

Figure A-2 – CRTF Assessment Statement.

A14. A verifiable list will be maintained on the NCSC Website providing information on products that have been assessed under the CRTF Scheme.

Additional Set-up and Onboarding Requirements

Requirements to Deliver CRT Assessments

A15. The CRTF team conducting the CRT evaluation and producing the reports shall include at least one member who has completed the *Performing Cyber Resilience Testing (PBA)* training course.

Trial Evaluation

A16. The Company must complete a CRT trial evaluation of a suitable Product, as described in Section 2, to provide evidence to the Accreditation Body (UKAS) that the Company complies

[12] The *Product Assessment Report* (PAR) Template will be issued separately to each CRTF.

[13] See section 3.4 for further details.

with ISO/IEC 17020 and demonstrate their ability to conduct a full CRT assessment including the production of the required output reports.

Product Assessment Reporting

A17. The Company shall follow the reporting guidance contained in Section 3 – Assessment Reporting Guidance and produce the *Product Assessment Report (PAR)* in accordance with the latest version of the Template issued by the Authority.

Annex B - Sanitisation Service Assurance

Introduction to Sanitisation

B1. Sanitisation refers to the process of treating data stored on Electronic Storage Media (ESM) to minimise the risk of retrieval or reconstruction. This is required in several scenarios, such as equipment reuse, disposal, or destruction.

B2. The service provides a framework for Service Providers delivering ESM asset sanitisation services to demonstrate how they meet the Sanitisation Assurance Service Standard.

B3. Sanitisation can be carried out through multiple methods, each selected based on the specific requirements of the client and the level of risk being addressed. These will include physical destruction of media and overwriting to render data irretrievable. The choice of method depends on factors such as Client's requirements, the classification level, and the intended future use of the asset. For example, highly classified ESM may require destruction, while ESM intended for reuse at the same classification tier may be overwritten.

B4. Examples of the sanitisation of ESM types covered within the scope of the NCSC's sanitisation guidance could include the following:

a. Non-destructive procedures applied to OFFICIAL Hard Disk Drives intended for re-use at the same classification tier.

b. Destructive procedures applied to SECRET Flash media.

c. A combination of non-destructive procedures, followed by destructive procedures, on TOP SECRET Hard Disk Drives.

B5. NCSC guidance covering sanitisation of ESM at OFFICIAL is published on the NCSC website[14]. NCSC guidance covering sanitisation of ESM at SECRET and above is available on request[15].

B6. The sanitisation of cryptographic items is outside the scope of this service. For information regarding the sanitisation of cryptographic items, please refer to HMG Standard

[14] Secure sanitisation and disposal of storage media - NCSC.GOV.UK

[15] Contact ncscindustryassurance@ncsc.gov.uk. Add "CRTF" to the beginning of the subject line.

number 4 which is available to Crypto Custodians via the COMSEC Compliance Team at cct@ncsc.gov.uk.

B7. Where legacy media classified under previous Government Classification Schemes is being processed, Service Providers shall come to an agreement with their Client on equivalency between old and new markings.

Summary of Service Requirements

B8. Services can be evaluated and reported on against the re-use and / or destruction of any ESM type and government classification covered within the scope of the NCSC's sanitisation guidance. Services covered can be those offering either or a combination of both destructive and non-destructive processes.

Location of Sanitisation Activities

B9. Service Providers will typically provide either or both of the following for the sanitisation of ESM:

a. Mobile Service – Services where the Service Provider has secure vehicles fitted with equipment that can perform sanitisation at the Client's own site or where items are transported using secure vehicles by the Service Provider for destruction at either their own or a third-party facility.

b. Fixed Site Service – Services where sanitisation is carried out on the Service Provider's site.

Health and Safety

B10. During the evaluation process it is likely that the CRTF Team will be required to work in proximity to the equipment used in the sanitisation process. The CRTF Team shall:

a. Ensure they have the appropriate safety gear for each activity and use it as instructed by the Service Provider.

b. Be accompanied and supervised whilst in high-risk areas on the Service Provider's premises, in accordance with applicable health and safety requirements.

c. Follow all safety instructions given by the Service Provider during their visit.

d. At no point operate machinery.

Sanitisation Evaluation Process.

Summary

B11. The Sanitisation evaluation process aligns with the core stages of the CRT evaluation process, while incorporating additional requirements specific to Sanitisation assurance.

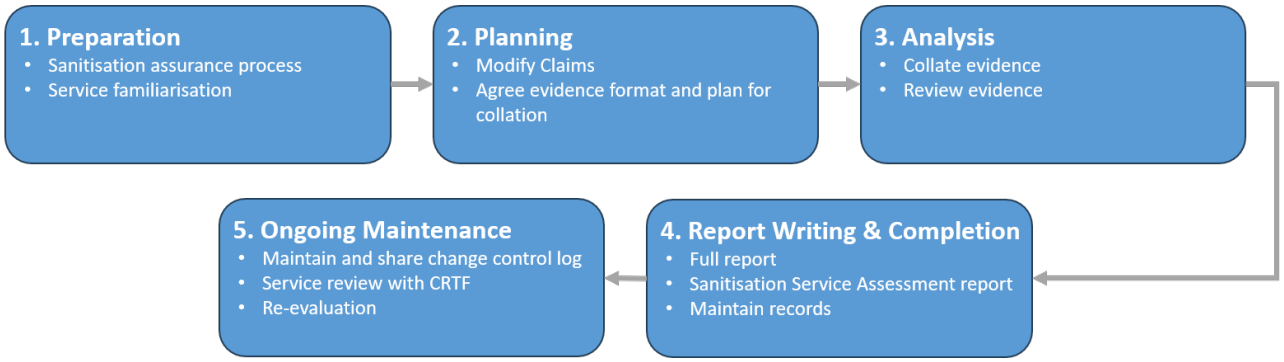


Figure B-1 – Sanitisation evaluation process.

B12. The CRTF Team performing the evaluation may have different roles. There shall be a lead who will be the primary point of contact with the Customer and will be responsible for the overall integrity of the evaluation. An experienced evaluator with knowledge of the specific service offering may perform most of the work.

Preparation

B13. The preparation phase shall ensure that:

a. All evaluations are conducted and owned by a certified ISO/IEC 27001 auditor or CISA (Certified Information Systems Auditor).

b. That the Customer has sufficient understanding of the evaluation and assessment process to complete the evaluation.

c. The CRTF has sufficient understanding of the sanitisation assurance process to conduct the evaluation.

B14. The CRTF will support the Sanitisation Service Provider throughout the evaluation process. This will include making the Service Provider aware of the requirements before starting the evaluation. The Service Provider may wish to start the evaluation knowing there may be gaps in their evidence which will result in Risks Identified in the *Assessment Report*. The CRTF can also support the Service Provider in identifying areas where they can

strengthen their evidence before the evaluation starts. This should be discussed and agreed between the CRTF and Service Provider.

B15. The NCSC actively encourages the re-use of current and valid evidence gained through other routes where this evidence meets the Claims required to demonstrate that a Service Provider meets the Sanitisation Assurance Principles.

Planning

B16. During the planning phase the CRTF shall:

a. Agree the Claims to be evidenced and where modifying Claims, ensure it is necessary, appropriate and supported by an appropriate PBA style argument.

b. Agree evidence requirements for each claim and identify gaps.

c. Create a plan for gathering evidence in the most appropriate manner. No single approach is likely to satisfy every situation.

d. Use effective tools to collate, manage, and share evidence.

Analysis

B17. During the analysis phase the CRTF shall:

a. Develop and use a consistent and repeatable approach to the process of collating and reviewing evidence.

b. Identify and categorise gaps in evidence as risks in accordance with the PBA methodology.

B18. The CRTF Team is required to witness the sanitisation process using an example of each type of ESM covered by the Service being evaluated.

B19. The CRTF Team shall perform evaluation activities sufficient to have confidence that each Principle has been examined and reported on where appropriate.

Report Writing and Completion

B20. Prior to the completion of an evaluation the:

a. CRTF and Customer are required to agree the format of the Full Report that will be issued only to the Customer. The report should enable the Customer to easily identify areas where the sanitisation services or working practices could be improved.

b. CRTF will ensure that the *Sanitisation Service Assessment Report (SSAR)* [16] adheres to the standard template provided.

c. CRTF is to advise the Customer that making the SSAR available to the end user of the service is a condition of the CRTF scheme [17].

d. CRTF will ensure that evaluation records are updated and maintained as required.

B21. On completion of a CRTF evaluation Sanitisation Service Providers may use the following tagline for use in their marketing and promotional materials:

NCSC CRTF – Cyber Resilience Assessed

Small print: Assessment conducted via an NCSC Cyber Resilience Test Facility (CTRF) does not imply compliance with regulatory standards, best practice, or any other form of certification.

Figure B-2 – CRTF Assessment Statement.

B22. A verifiable list will be maintained on the NCSC Website providing information on sanitisation services that have been assessed under the CRTF Scheme.

B23. A Service Provider may choose to use products and services certified by other assurance schemes to provide additional confidence to their clients. The NCSC has no objection to these being identified in the *Sanitisation Service Assessment Report (SSAR)*. If these certified products and services are listed, the assurance scheme used shall also be identified along with any certification expiry date or a link to the certification details.

Ongoing Maintenance of the Sanitisation Services

[16] The *Sanitisation Service Assessment Report (SSAR)* Template will be issued separately to each CRTF.

[17] See section 3.4 for further details.

B24. For Sanitisation Service Assurance there is a requirement to maintain the service and ensure the Client is aware of changes that may impact the suitability of the service to meet their specific requirements. This is reflected with an additional stage to the evaluation process.

B25. The Service Provider will maintain a detailed and proactive change control log, incorporating a clear treatment plan for any issues identified during evaluations. This documentation should accompany the Sanitisation Service Assessment Report (SSAR), demonstrating commitment and transparency to continuous improvement and rigorous change management. Clients shall be kept informed of relevant and significant updates to gain assurance that the Service remains aligned with their evolving needs. Ongoing enhancement and diligent maintenance are core pillars of the Sanitisation Service that support the Client's requirement for secure end of life management of their data.

B26. Re-evaluation of the Service will be required under certain circumstances, initiated either by the Service Provider or the Client. This should be in response to changes that impact service delivery or the time elapsed since the last evaluation. While updates are tracked in the change control log, a formal re-evaluation provides a more thorough review and integrates these changes into a refreshed, contemporary Assessment Report offering clearer insights for the Client. It is expected that the Service Provider will conduct a service review with a CRTF either annually or whenever a significant change[18] is introduced. The CRTF will advise whether a re-evaluation is a proportionate step to maintain Client confidence in the Service.

Additional Set-up and Onboarding Requirements

Requirements to Deliver Sanitisation Assessments

B27. The CRTF team conducting the Sanitisation Service evaluation and producing the reports shall include at least one member who has completed the Performing Cyber Resilience Testing (PBA) training course.

Trial Evaluation

B28. The Company must complete a Sanitisation Service Assurance trial evaluation of a suitable Service, as described in Section 2, to provide evidence to the Accreditation Body (UKAS) that the Company complies with ISO/IEC 17020 and demonstrate their ability to

[18] Examples of significant change could be – but not limited to - a new shredder, processing location, change in scope of material that could be processed, or company acquisition. The Service Provider should be guided by the CRTF.

conduct a full Sanitisation Service assessment including the production of the required output reports.

Sanitisation Assessment Reporting

B29. The Company shall follow the reporting guidance contained in Section 3 – Assessment Reporting Guidance and produce the *Sanitisation Service Assessment Report (SSAR)* in accordance with the latest version of the Template issued by the Authority.

Last Page