National Cyber Security Centre
a part of GCHQ

Assured CHECK Scheme Buyer's Guide

V1.1 December 2024

Document history

Date	Version	Change history details	POC
26/03/2024	1.0	Final Version Issued as a letter for CHECK companies to distribute to Buyers.	CHECK Scheme Management Team
10/12/2024	1.1	Letter format changed to document format to aid version control. Guidance added for Buyers working in specialist/operational technology environments.	CHECK Scheme Management Team

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

Document owner

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

Abbreviations and definitions

CHECK Scheme Standard	Means the standards which must be met to be part of the CHECK scheme. Referred to as the Standard.
CHECK Team Leader (CTL)	Means the NCSC-approved Company staff member appointed as a team leader to lead teams during CHECK services.
CHECK Team Member (CTM)	Means the NCSC approved Company staff member appointed to assist a CHECK Team Leader with the delivery of CHECK services.
Company	Means the company which is, or is applying to become, a CHECK scheme member.
Customer	Means the organisation which contracts with the Company for CHECK services.
Primary CHECK Team Leader	Means the CHECK Team Leader who is accountable for each CHECK penetration test and is contactable for the duration of the testing.
We/Us/Our	Means the NCSC.
You/Your	Means the Customer.

Introduction

1. This document provides guidance and clarity around the NCSC's Assured CHECK Penetration Testing Scheme and highlights how we would expect you, the Customer, to engage with services assured under CHECK.

2. Please send any feedback or suggestions for additional content to ncscindustryassurance@ncsc.gov.uk.

What does NCSC-Assured mean?

3. We have assessed that all companies which are members of the NCSC's Assured CHECK Penetration Testing Scheme meet our Scheme standards. Broadly speaking, these standards cover:

   a. The technical competence of individuals conducting the tests.

   b. The Company's adherence to the NCSC's penetration testing methodology.

   c. The Company's ongoing commitment to service improvement and continuous development of its staff.

   d. Basic due diligence around the Company's financial and security status. This means that we check:

      i. whether the Company or its officers have been convicted of certain offences which might constitute mandatory grounds for exclusion from government contracts (such as convictions for fraud or tax evasion).

      ii. the "risk indicator" for the Company's Dun and Bradstreet Rating (D&B Rating, as explained here: https://www.dnb.co.uk/about-us/our-analytics/predictors-scores-ratings/scores-ratings.html). However, depending on a Company's circumstances and any possible mitigations, a higher risk indicator (3 or 4, or where there is insufficient information to assign an indicator) will not necessarily exclude it from the Scheme. This is only a basic creditworthiness check made when a Company joins the Scheme and potentially at periodic points thereafter, but in each case, it

only gives a snapshot of the Company's financial risk at the time at which it is performed. It remains your responsibility to perform all financial due diligence that is necessary and appropriate to your relationship with the Company.

iii. that all CHECK Team Leaders and CHECK Team Members hold a minimum of SC clearance. However, we do not sponsor all of the clearances. It is your responsibility to assure yourself that clearances are valid and acceptable to your organisation. You may do this either by checking with the United Kingdom Security Vetting (UKSV) team or, where GCHQ sponsors the clearance, by emailing ncscindustryassurance@ncsc.gov.uk. Please allow as much time as possible to conduct these checks, owing to resource constraints in both teams. In addition to these clearance checks, the NCSC reserves the right to carry out background security checks (which might include checking for potential reputational impact on the NCSC) on a Company (and, in some cases, those checks may result in exclusion from the Scheme). However, any additional checks carried out are likely to be context-specific and will only assess risk at the time at which they are made (which, as with ii. above, is the point when the Company joins the Scheme and potentially at periodic points thereafter), so you should not rely on a Company's status as a CHECK member as being a guarantee on the NCSC's part that your use of that Company will be risk-free from a security perspective. If you have any particular security concerns, please contact the NCSC for help at ncscindustryassurance@ncsc.gov.uk

iv. that the Company has a Cyber Essentials Plus certificate.

4. We assess companies on joining the scheme and randomly sample their work throughout the year to ensure that they continue to meet our standards.

5. We meet regularly with the CHECK community for knowledge sharing and feedback purposes.

6. The CHECK Scheme Standard and associated documents are all available on the NCSC's website Scheme documents - NCSC.GOV.UK. We strongly encourage you to familiarise yourself with the contents so that you know what to expect from a CHECK Company. However, for ease, and in response to feedback from our community, we would like to highlight a number of expectations regarding how you should engage with the assured services, which will enable your CHECK engagement to proceed smoothly.

Specialist and Operational Technologies

7. If you are a buyer of CHECK services in, for example, CNI or specifically regulated sectors, you may need to find CHECK Companies with knowledge and experience of specialist or bespoke technologies, such as operational technologies and related embedded systems.

8. We have not assessed any CHECK Company's ability to research and analyse such technologies. Some CHECK Companies may have relevant, specific knowledge and experience to meet your requirements, but you should put in place additional steps to verify any claims made by prospective suppliers. You should also consider whether you need additional support from a third party such as the vendor or specialist provider of your technologies.

Customer Expectations

9. During the Scoping phase, to obtain the full benefit of the assured service, you must:

    a. provide all available supporting system security procedures and security architecture documentation (eg a network topology), and a current vulnerability assessment report, if available.
    b. outline any issues which might impact on testing, for example the need for out-of-hours testing, or special handling restrictions for critical systems.
    c. agree a realistic amount of time for the engagement to enable a thorough test.
    d. have Business Continuity Plans in place.

e. clearly articulate your data handling requirements in respect of your data and vulnerability information.

10. Before the test start date, to obtain the full benefit of the assured service, you must have:

    a. completed all steps to meet the penetration testing team's requirements, such as creating test accounts, issuing and checking certificates or allocating desk space.
    b. identified relevant staff who can be contacted by the Company Primary CHECK Team Leader for the duration of the engagement.

12. After completion of the test, to obtain the full benefit of the assured service, you must:

    a. verify that, as far as possible, the CHECK Team has removed all artefacts created as a result of testing from your system, and/or that you have acted to clean up any outstanding artefacts.

    b. respond to any request to provide feedback on the CHECK Company's work, whether that request is from the Company itself or from the NCSC. You are welcome, at any time, to provide feedback independently by emailing ncscindustryassurance@ncsc.gov.uk.

13. While not strictly part of the CHECK Scheme standard, we strongly encourage you to view a CHECK penetration test as a tool to improve the security of your organisation, rather than as a 'tick-box exercise'. As a result, your CHECK report will be structured in such a way that you can plan your remediation activities.

Submission of CHECK reports to the NCSC

14. All CHECK scheme members are contractually obliged to submit CHECK reports on systems below SECRET to the NCSC, using our secure portal. As a result, they are obliged to include that requirement in their contract with you. For all tests

on systems classified SECRET and above, you must retain those reports and make them available to the NCSC on request.

15. All reports submitted to the NCSC are held within our secure repository, to which only authorised people have access and only for the specific purposes in paragraphs 16a and 16b.

16. Feedback from CHECK companies suggests that some customers do not understand the NCSC's rationale for collecting reports and are uncomfortable about allowing their release to the NCSC. We hope that the following provides reassurance but are happy to discuss further:

    a. For quality assurance purposes and to maintain standards, we need to regularly assess the work produced by the CHECK member companies, as outlined in paragraph 3. Accessing reports in the repository allows us to do the assessment in a timely fashion and to pick representative samples of work. The results of these activities remain confidential between the NCSC and the CHECK Company.

    b. In our role as the National Technical Authority for Cyber Security, we need to establish and monitor trends and highlights across Central Government, Critical National Infrastructure and the Public sector. We can use the CHECK reports to collate information on vulnerabilities and the state of the UK's infrastructure as a whole. This allows us to put out more tailored advice, or to commission work which might help to resolve widespread issues. Such research is done by our in-house data science team and no raw data is released outside of the NCSC. In addition, all results are anonymised so that no specific organisation can be identified. Under no circumstances will we use the information within CHECK reports to 'name and shame' individual organisations.