National Cyber Security Centre
a part of GCHQ

Assured CHECK Scheme Standard

V1.1 November 2024

Document history

Date	Version	Change history details	POC
26/03/2024	1.0	Final Version	CHECK Scheme Management Team
07/11/2024	1.1	Change in qualification criteria for CHECK Team Leaders and CHECK Team Members. (Removing 'approved exams' and replacing with UK Cyber Security Council Titles) Paragraph 16c updated to give some flexibility around the identification and responsibilities of a Primary CHECK Team Leader during the scoping meeting. Paragraph 37c updated to give limited flexibility on CHECK report authors. Paragraph 37g added a requirement to use neutral language in report writing. Correction of typos.	CHECK Scheme 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 and definitions

Agreement	Means the Ecosystem Agreement between the NCSC and CHECK Company, including all Schedules, as amended from time to time.
Assured Service Provider Logo	Means the Assured Service Provider Logo as issued by the NCSC.
Assured 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.
CHECK Test Team	Means the team of qualified individuals carrying out a CHECK penetration test on a Customer's system
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.
Service Owner (SO)	Means the person in the company with overall responsibility for the CHECK scheme offering.
Technical Lead (Tech Lead)	Means the person in the company responsible for the technical delivery of CHECK services.
We/Us/Our	Means the NCSC.
You/Your	Means the company which is, or is applying to become, a CHECK scheme member.

About the CHECK scheme

Scheme membership requirements

1. This document defines the standards required for membership of the CHECK scheme. It is split into three sections:

    - The Company Standard – Section A
    - The Technical Testing Methodology – Section B
    - The Report Writing Standard – Section C

2. You must read this Standard in conjunction with the CHECK scheme 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 CHECK penetration tests.

Section A – The Company Standard

Network security

3. 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

4. You must carry out 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 carried out.

    - Business requirements – "CHECK Service Owner"
    - Technical Health of the Company's CHECK service – "CHECK Technical Lead"
    - Technical Oversight of individual tests - "CHECK Team Leader"

5. All CHECK Team personnel (CTLs, CTMs, Technical Leads, and any named CHECK Business Support staff) must be either permanent employees or sub-contractors and not employed or contracted for CHECK-related work by any other CHECK company.

CHECK Service Owner (SO)

6. While we do not expect one person to personally deliver all aspects of the CHECK service, the named Service Owner must be directly accountable for delivery of the Service as a whole. 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 CHECK community. This includes:

- contributing to CHECK 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 of its obligations under this Standard and the associated Agreement.

d. Submitting, on time, an annual Management Information Report to the NCSC. (A template will be provided.)

e. Documenting and maintaining Company Quality Management processes as they apply to the CHECK scheme.

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

g. Ensuring that everyone involved in the CHECK 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 on the CHECK Supplier portal, in particular of new CHECK Team Members and CHECK Team Leaders.

j. Ensuring the Company's contract with the Customer includes a contractual right to provide the NCSC with a copy of the CHECK report. The Customer must understand that this is the Company's contractual obligation to the NCSC under the CHECK scheme. The Customer must retain all protectively marked reports and make them available to the NCSC on request.

k. Actively monitoring and managing Customer relationships and seeking Customer feedback to provide evidence of Customer satisfaction with the Company's work.

CHECK Technical Lead

7. The named Technical Lead must be directly accountable for the technical health of the CHECK service. We would normally expect the Technical Lead to be an experienced penetration tester, but this is not mandatory. However, the individual must have the capacity and capability to sign off all of the following mandatory tasks:

    a. Acting as the NCSC's primary contact for all technical feedback and questions regarding the technical aspects of the CHECK service, and any onward action required. This includes acting on NCSC feedback on CHECK reports.

    b. Ensuring the technical quality and standard of delivery of the CHECK service and maintaining the overall technical health of the CHECK team.

    c. Accountability for the quality of reports, ensuring they meet both the CHECK Standard and the Company's standards. We do not expect the Technical Lead to personally quality control every report, but we do expect the company to have and adhere to a quality control process, for which the Technical Lead is accountable.

    d. Ensuring all CHECK Team Leaders and Members have appropriate professional training and development plans. This may include:

        - identifying mentors for inexperienced CHECK Team Leaders/Members
        - ensuring there is a training lead for CHECK Team Leaders
        - ensuring all CHECK Team Leaders attend at least two NCSC masterclasses or events per year

    e. Accountability for checking all CHECK Team Leader and Member applications against the Standard, and approving them, before they are passed to the NCSC.

UK Cyber Security Council Professional Standards

8. The UKCSC is the self-regulatory body for the UK's cyber security profession. It develops, promotes and stewards nationally recognised standards for cyber security in support of the UK Government's National Cyber Strategy. The NCSC uses the UKCSC's 'Security Testing' specialism framework to define the professional standards required for a CHECK Team Leader and CHECK Team Member.

CHECK Team Leader

9. CHECK Team Leaders must:

    a. have achieved a UKCSC Security Testing Title at the 'Principal' level, as a minimum.
    b. hold a minimum of SC clearance.
    c. be a permanent employee and not employed by any other CHECK company.
    d. have a track record of satisfactory Customer engagement.

CHECK Team Member

10. All CHECK Team Members must:

    a. have achieved a UKCSC Security Testing Title at the 'Practitioner' level.

    b. hold a minimum of SC clearance.

Composition of a CHECK Test Team

11. All CHECK Test teams must meet the following requirements:

    a. Comprise only NCSC registered CHECK Team Leaders and CHECK Team Members.

    b. Comprise the appropriate mix of expertise for the component technologies of the target system.

    c. Hold whatever clearance is required by the Customer.

    d. Include a named Primary CHECK Team Leader who:

        - is qualified in the relevant discipline for the test.
        - is accountable for the engagement.
        - must be contactable by all members of the testing team and by the customer for the duration of the engagement.
        - is responsible for the behaviours, actions and advice given by their team.
        - is responsible for conducting the test in accordance with the CHECK Methodology (Section B).
        - is responsible for producing the final report in accordance with the CHECK Report Standards (Section C).

Section B - CHECK technical testing methodology

12. All CHECK companies must operate according to the methodology below.

Scoping

13. The Company must agree with the Customer the scope of the penetration test. This must include identification of:

    a. the system itself.

    b. the threats (and threat agents) to be countered.

    c. the system's component technologies, products and configuration.

    d. the types of test.

14. The Customer is expected to provide the Company with all available supporting system security procedures and security architecture documentation (eg a network topology), and a current vulnerability assessment report, if available. This will not preclude the Company from investigating threat scenarios where threat agents do not have direct access to such documentation or information.

15. If the Customer asks for a test which the Company knows is inappropriate (that is, it will not help the Customer understand their vulnerability status), the Company must explain this to the Customer and suggest an alternative way forward. If the Customer wishes to continue regardless, the Company must record the advice given and the Customer's decision in the CHECK report. By way of example only, a test scheduled at the wrong stage of a project would be inappropriate.

The scoping meeting

16. The scoping meeting between the Company and the Customer must involve:

    a. all relevant risk owners – must outline any areas of special concern.

    b. technical staff knowledgeable about the target system – must outline the boundaries of the organisation's IT estate.

    c. the Primary CHECK Team Leader is responsible for identification of what testing they believe will give a full picture of the vulnerability status of the system. If the Primary CHECK Team Leader has not been identified at the time of the scoping meeting, a CHECK Team Leader must fulfil this responsibility. This CHECK Team Leader is subsequently responsible for ensuring all relevant information is given to the Primary CHECK Team Leader undertaking the engagement. Typically, this will include:

        i. components at risk from the specified threats.

        ii. components considered by the Company to be particularly vulnerable (in respect of either their construction or supporting system security procedures).

        iii. components in which the Customer has least confidence at the start of the penetration test.

        iv. description of the tools the Company is planning to use so that the Customer understands the tools are safe and have been acquired from trusted sources.

17. The Company must understand the Customer's data handling requirements in respect of their data and vulnerability information.

18. The Company and the Customer must agree a realistic amount of time for the engagement to enable a thorough test.

Special requirements

19. The Customer must outline any issues which might impact on testing, for example the need for out-of-hours testing, or special handling restrictions for critical systems.

20. Where the Customer does not want certain critical system elements to be tested (for example on account of operational risk), the Company must seek other means of assessing their security, for example by confirming release and patch numbers of the associated components and comparing those to relevant vulnerabilities.

21. The Company must discuss any remote access arrangements, including any security implications with the Customer.

22. The Company must make the Customer aware that no security testing is without risk and ensure that the Customer has Business Continuity Plans in place.

Test preparation

The Company

23. The Company must formulate a test strategy in keeping with the agreed scope.

24. As a minimum and as appropriate within the agreed scope, the test strategy will typically include:

    a. External Threat Agents scenario:

        i. attempting to gain electronic access to a target node

ii. attempting to gain identity credentials for that node

b. Internal Threat Agents scenario:

i. attempting to gain extra privileges for an (assumed or gained) identity

ii. attempting to defeat auditing and detection mechanisms

iii. attempting to defeat other security mechanisms, for example access control

c. Network Threat Agents scenario:

i. attempting to move on to other network nodes

ii. attempting to move on to other networks

25. When considering the level of testing, the Company must give priority to those areas where risks are considered to be greatest.

26. The Company must test for all obvious potential vulnerabilities within the agreed scope.

a. Annex A illustrates what this means for Infrastructure testing.

b. Annex B illustrates what this means for Web Application testing.

The Customer

27. Before the test start date, the Company must ensure that the Customer has:

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 CTL for the duration of the engagement.

Test execution

Process and procedure

28. The Company must not deliberately damage the system under test and must use all reasonable endeavours to minimise accidental damage to the system under test.

29. The Company must keep the test strategy under review during the testing.

30. The Company and Customer must maintain contact during the test execution, so that both parties are aware of what specific tests are being performed.

31. If additional tools are required, to those proposed during scoping, the Company must discuss them with the Customer prior to use so that they understand they are safe and from trusted sources.

32. The testing must respect the data handling requirements agreed during scoping. In particular, no sensitive client data will be removed from the Customer's network except that which will form part of the report.

Technical

33. The Company must test each threat, identified in the agreed scope, for each major system component, following the test strategy.

34. Any sampling undertaken must be appropriate to the system under test and to the criticality of individual components.

Post test clean-up

35. As far as possible, the Company must remove all artefacts created as a result of testing from the Customer's system. The Company must make the Customer aware of their responsibility to verify that the clean-up has taken place and/or to act to clean-up any outstanding artefacts.

36. After the Customer has confirmed receipt of the report, the Company must erase all test data, or transfer the data to a secure internal repository for a period in line with regulatory and legal requirements, including data protection laws. The Company must complete this work within a reasonable period, as agreed by both parties.

Section C

CHECK reporting standard

37. All CHECK reports must adhere to the following standards:

Overall

a. The CHECK Assured Service Provider – CHECK Penetration Testing logo must be clearly displayed.

b. A point of contact and contact details for the CHECK Customer organisation must be included.

c. The report may be written either by the Primary CHECK Team Leader or by a CHECK Team Leader who was part of the test team. In both cases, the report must be signed off by the Primary CHECK Team Leader. The name of the author and the Primary CHECK Team Leader must be in the report.

d. The report must not contain any sensitive data (as determined by the Customer), passwords or any Personally Identifiable Information (PII).

e. The report must contain an Executive Summary, directed at a non-technical audience. The Executive Summary must include:

i. an explanation of how the penetration tests performed met the requirements of the scope agreed with the Customer.

ii. a summary of the overall security posture of the system tested and the highest level of vulnerability impact achieved.

iii. a summary of the key technical findings and statement of their impacts.

iv. a summary of the key recommendations, which are relevant to the Customer's environment, context and any relevant restrictions.

f. The report must be structured in such a way that the customer can plan their remediation.

g. The author must always use neutral language, for example ‘allow/deny list’ rather than ‘white/black list’.

38. From this point, the report can be exclusively directed at a technical audience if desired.

Report preliminaries

39. The report must communicate the scope of the task and include all of the following:

a. the reason for and context of the test.

b. the aim of the task (as agreed with the Customer during scoping).

c. the dates of testing.

d. identification of the hosts and devices, or address ranges agreed with the Customer as specifically in or specifically out of scope.

e. an explanation of any strategy to reduce the ideal scope of the task (e.g. representative sampling).

f. an explanation of any changes to the test boundaries which occurred during the test.

g. other Customer-imposed restrictions that affected testing.

Vulnerability reporting

40. All vulnerabilities must be accurately identified and described as follows:

a. you must positively confirm the presence of a vulnerability whenever possible and minimise generalisations.

b. you must describe the potential impact of all identified vulnerabilities, as appropriate to the Customer's environment, context and any relevant restrictions.

c. you must assess the severity of a vulnerability as described in paragraph 37 and explain any reduction in severity rating.

d. you must clearly identify hosts affected by each vulnerability, including relevant TCP or UDP port numbers where applicable. Where the list is too long or complex for inclusion in the main body of the report, you must list the affected hosts in an appendix.

e. you must group together vulnerabilities falling into the same type or class.

Severity ratings

41. CHECK reports must state the level of risk as HIGH, MEDIUM, LOW or INFORMATIONAL. In addition to (but not in place of) this rating, you may also use the Common Vulnerability Scoring System (CVSS).

42. You must determine the level of risk by combining your knowledge of the severity of the vulnerability (the CVSS score), with the impact on the Customer if that vulnerability were exploited, and your knowledge of mitigations or other controls in place.

Vulnerability recommendations

43. You must provide a solution for each vulnerability identified. You must:

a. be accurate.

b. refer to technical controls and describe them in procedural form wherever possible.

c. provide resources containing further information on a vulnerability.

d. be impartial and not favour the products of any particular vendor, paying attention to value for money.

e. be relevant to the Customer's environment, context and any relevant restrictions.

f. generally avoid blanket recommendations.

g. provide alternative, appropriate recommendations in the event that the full solution cannot be implemented within a reasonable timeframe.

Annex A – Infrastructure testing

44. During any infrastructure testing engagement, as a minimum, you must include the following in your evaluation:

    a. Network mapping – defined as “the process of creating an inventory of devices connected within a network to understand the structure and layout of that network”.

    b. Port scanning – defined as “a technique used to identify open ports on a computer system and analysing the responses to determine which ones are active and accessible”.

    c. Service enumeration – defined as “the process of identifying and gathering information about services running on a target host or network”.

    d. Vulnerability assessment – defined as “the process of identifying, classifying, and prioritising vulnerabilities in a computer system, application, or network”.

    e. Exploitation of vulnerabilities – defined as “the process of taking advantage of weaknesses in a system, application, or network to achieve goals unintended by the computer system / network owner”.

    f. Post Exploitation Activity – defined as “activities a real attacker would use to maintain persistence, escalate privileges, move laterally, and exfiltrate sensitive data”.[1]

[1] The definitions of terms a to f are based upon those generated using Perplexity's pplx-7b-online Large Language Model.

45. The Company must test each mode of attack associated with a given threat (modes of attack might include monitoring communications, brute force, exploitation of bugs and loopholes).

46. The Company must test each parameterisation of a given mode of attack (for example, a representative selection of weak passwords).

47. The Company must test the configuration of system components for security.

48. The Company must test trust relationships between networks/nodes governed by different security procedures.

49. The Company may use automated vulnerability scanning tools (such as password crackers, port scanners, network discovery software, and vulnerability scanners) to maximise test coverage. However, as Customers rely on the Company's interpretation of the tool results in the context of the agreed scope, heavy reliance on such tools without providing sufficient interpretation will not meet CHECK standards.

Annex B – Web application testing

50. During any web application testing engagement, as a minimum you must include the following in your evaluation:

    a. API/Endpoint enumeration – defined as “the process of discovering and cataloguing all accessible endpoints in a web application”.

    b. Vulnerability assessment – defined as “the process of identifying, classifying, and prioritising vulnerabilities in a computer system, application, or network”.

    c. OWASP Top 10 Security Risk – defined as “an evaluation of “OWASP Top 10 Web Application Security Risks” as defined at OWASP Top Ten | OWASP Foundation

    d. Exploitation of vulnerabilities - defined as “the process of taking advantage of weaknesses in a system, application, or network to achieve goals unintended by the computer system / network owner”.

    e. Post Exploitation Activity - defined as “the activities a real attacker would use to maintain persistence, escalate privileges, move laterally, and exfiltrate sensitive data”.[2]

51. You must run tests with different user roles, since the system may behave differently with respect to users having different privileges.

52. You must run tests to explore Cross Site Request Forgery and Cross Site Scripting attacks, including with different user roles.

[2] The definitions of terms a to e are based upon those generated using Perplexity's pplx-7b-online Large Language Model.

53. Typically, an application security test is a directed assessment of an application and associated platform, this can include the:

    a. Application

    b. Application server

    c. Application database server

    d. Application client software and system

    e. Application communications

54. Testers must ensure that they have access to the underlying infrastructure to evaluate security weaknesses within the operating system, paying particular attention to misconfigurations, such as excessive privileges or permission issues.