National Cyber Security Centre

Version 2.0

April 2025

Willow

Introduction

This booklet contains the question set for the Cyber Essentials Plus information assurance standard:

Answering the questions

The booklet is intended to help you to understand the questions and take notes on the current setup in your organisation. In order to complete the assessment, you must enter your answers via IASME's online assessment platform.

You must answer all questions in order to achieve certification.

Your answers must be approved by a Board level representative, business owner or the equivalent, otherwise certification cannot be awarded.

Need help?

If you need help with understanding the questions, get in contact with IASME on +44 (0)3300 882752 or email info@iasme.co.uk

Alternatively, IASME has a network of Certification Bodies who are skilled information assurance companies who can provide advice on the standards and who can help you make changes to your setup in order to achieve compliance. Visit the IASME website at www.iasme.co.uk to find your nearest Certification Body.

Scoping

To clarify the scope of the assessment.

0.1 Have you verified that the scope for this CE+ assessment is the same as the scope for the applicant's CE verified self assessment (VSA)?

[Notes]

0.2 Provide a brief summary of the networks and locations in scope for this CE+ assessment.

[Notes]

0.3 If you have chosen to exclude any items, please provide a summary.

For example: "Company Website is excluded because it is located with the cloud hosting provider, and as such not required, as per the Cyber Essentials Plus scoping requirements"

If anything is excluded from the verified self assessment (VSA) in this CE+ assessment, then the VSA will need to be assessed again or the issue remediated within the prescribed 30 day window.

[Notes]

0.4 What is the name of the applicant?

Please provide the organisation's full name, to match that provided for their CE verified self assessment.

[Notes]

0.5 What is the CE verified self assessment (VSA) Blockmark certificate number for the applicant?

Please provide the certificate number for the client's CE self assessment questionnaire.

[Notes]

0.6 What date did the client pass their verified self assessment (VSA)?

Provide the date that the client passed their verified self assessment.

Cyber Essentials Plus must be completed within 90 days of the date of certifying for Cyber Essentials.

The 30 day remediation period is inclusive of the 90 days.

The CE+ assessment should be completed as close as possible to the date of the Cyber Essentials verified self assessment certification date, and sufficient time must be allowed for the remediation period within the 90 days.

Extensions will only be granted in extreme circumstances. This does not include Christmas, Easter or other publicly notified holidays, the dates of which are static or known in advance.

[Notes]

0.7 On what date/s was the CE+ assessment carried out?

If you have previously achieved Cyber Essentials, please select "Renewal". If you have not previously achieved Cyber Essentials, please select "First Time Application".

[Notes]

0.8 What is the scope description that should appear on the CE+ certificate?

The CE+ Scope must match the CE verified self assessment scope.

This must be the same scope description as the organisation's CE verified self assessment certificate. If the scope is the whole organisation please enter "Whole organisation".

[Notes]

0.9 Which CE+ Testing platform have you used, to run the email audit tests?

[Notes]

0.10 Was the CE+ audit carried out remotely or onsite?

[Notes]

0.11 Which vulnerability scanning tool was used for the external and internal audit? Was it supplied by the Certification Body or the applicant?

[Notes]

External Test

To identify all active IP addresses in use by the applicant and assess any potential vulnerabilities. Where dynamic IP addresses are in use for an Internet connection, the scope may be defined in terms of appropriate DNS entries. Take care with such addresses to ensure services like carrier-grade NAT do not inadvertently send assessment traffic to the wrong destination.

1.1.1 Does the scope of this assessment cover your whole organisation? Please note: Your organisation is only eligible for free Cyber Insurance if your assessment covers your whole company, if you answer "No" to this question you will not be invited to opt in to the included insurance.

[Notes]

1.1.1.1 Have you checked all external addresses against the networks and network devices in the CE VSA?

You must check against the answers given in Section 2 of the VSA. Please list the quantity of external IPs tested. Where it is unclear how many external IP addresses were tested, the quantity should be clarified with the applicant.

[Notes]

1.1.2 Did you identify any vulnerabilities that were scored 7 or higher on CVSS

The CVSS v3 is taken from the base score, and temporal scoring should not be taken into account.

[Notes]

1.1.2.1 Please provide a summary of all identified vulnerabilities.

The list should include a brief name of the vulnerability, its score and details of the affected device.

[Notes]

1.1.2.2 Has the client now addressed the high risk or critical vulnerabilities that were identified?

If there are vulnerabilities identified, the client must remediate the vulnerabilities and the identified service must be retested by the CE+ assessor within the 30 day remediation window.

Assessor notes are required about the remediation actions taken.

[Notes]

1.1.3 For each internet-accessible service you discover you must use the flow diagram in the Cyber Essentials Plus Test Specification document. Did the flow chart highlight any vulnerabilities as a fail?

[Notes]

1.1.3.1 Has the client now addressed the vulnerabilities that the flow chart identified as a fail?

If there are vulnerabilities identified, the client must remediate the vulnerabilities and the identified must be retested by the CE+ assessor within the 30 day remediation window.

Assessor notes are required about the remediation actions taken.

[Notes]

1.1.4 Please provide information about the remediations carried out including the date that they were retested.

[Notes]

Authenticated Vulnerability Scan

To identify missing vulnerability fixes within the defined CE+ test scope that could be exploited within the bounds of the CE threat model. Vulnerability fixes include patches, updates, registry fixes, configuration changes, scripts or any other mechanism prescribed by the vendor to fix a known vulnerability.

2.1.1 Has a suitable sample of all end user devices, servers and IaaS instances been identified, in line with Cyber Essentials Plus scheme guidance?
*The sample must be selected by the CE+ assessor **not** the applicant.*

The sample must be 100% representative of the applicant's infrastructure.

[Notes]

2.1.2 You must provide a brief summary of your device sampling decision.
Sample calculation data must be retained by the certifying body for the lifetime of the certificate.

[Notes]

2.1.3 Has a full authenticated vulnerability scan been conducted on all devices in your sample?

[Notes]

2.1.3.1 Where a vulnerability scan was not possible, has a manual check been carried out?

[Notes]

2.1.4 Did you identify any vulnerabilities for the tested devices that were scored 7 or higher against CVSS v3 scoring?
The CVSS v3 score is taken from the base score, and temporal scoring should not be taken into account.

[Notes]

2.1.4.1 Do any of the vulnerabilities identified in the internal vulnerability scan relate to issues for which a vulnerability fix has been made available by the software vendor (and was released more than 14 days ago)?

Only vulnerabilities for which the vendor has released a vulnerability fix, and the client has failed to install the fix will cause a fail for this test. If you identify a high risk or critical vulnerability for which a vulnerability **HAS NOT** been released, you should answer NO to this question (which will result in a PASS for the client).

[Notes]

2.1.4.2 Please list the vulnerabilities for which a vulnerability fix has been released.

When vulnerabilities have been identified, a summary list must be provided.

[Notes]

2.1.4.3 Has the applicant applied the vulnerability fixes to address the identified vulnerabilities? Please provide notes on what happened.

If there are vulnerabilities identified, the client must remediate the vulnerabilities and the identified service must be retested by the CE+ assessor within the 30 day remediation window.

[Notes]

2.1.5 Please provide information about the remediations carried out including the date that they were retested.

[Notes]

Malware Protection

Perform this test on sampled end user devices, servers that provide a user-interactive desktop and IaaS instances to check that all the devices in scope benefit from at least a basic level of malware protection.

3.1.1 Has a suitable sample of all end user devices, servers and IaaS instances that provide a user-interactive desktop been identified in line with Cyber Essentials Plus scheme guidance?

You must use the same devices as picked in the sample for the authenticated vulnerability scan.

VDI Servers, Virtual desktop servers, DaaS servers must be tested.

All other servers do not need to be tested.

[Notes]

3.1.2 For all end user devices in the sample, have you identified which method of preventing malware is in use? Please select every method that is in use at this organisation.

The methods of preventing malware available are:

A - having anti-malware software installed

Or

B - limiting installation of applications to an approved set (i.e. using an App Store and a list of approved applications)

3.1.3 Which email domain/s have been tested?

List the email domains.

[Notes]

3.1.4 How many individual email addresses have been tested?

List the quantity per email domain tested.

[Notes]

3.1.5 Please provide information about the remediations carried out including the date that they were retested.

[Notes]

Malware Protection Using Anti-Malware Software

3.2.1 For all devices in the sample relying on A - anti-malware software, is antivirus software installed on all end user devices or virtual desktop environments?

[Notes]

3.2.2 For all devices in the sample relying on A - anti-malware software, determine whether the test files will work for the testing purpose.

Test files must be used to test all anti malware software that uses signature based scanning.

Determine whether the test files should be triggered using the software installed and then answer one of the following options:

A - Test files work on all sampled devices

B - Test files do not work on any device within the sample set

*C - Test files work on **some** of the devices in the sample set*

[Notes]

3.2.3 For all end user devices in your sample using anti malware software that should defend against the test files, have you tested email delivery by sending a test email with no attachments and verified the receipt of the email?

[Notes]

3.2.4 Have you sent a suitable set of test files by email to each device in the sample (this should include "malware" test files and "executable" test files)?

You must use the standard test files provided by IASME to carry out this test. You only need to send a subset of these files that would be appropriate to the device operating system (for example, Windows devices do not need to be sent the .dmg file, which is a macOS file). There are two types of test files - "malware" and "exectuable". Both types must be sent to every device in the sample. If in doubt, please verify your list of test files with IASME. You should send one email per file.

[Notes]

3.2.5 Were all of the email attachments containing malware blocked by all of the end user devices in your sample?

You should answer No if you were able to open any of the malware attachments.

[Notes]

3.2.5.1 Has the client now addressed the configuration issue that allowed the malware to be opened? Please provide notes on what happened.

If you identify a configuration issue, the client may be given an opportunity to address the issue and have a retest of a specific device carried out.

[Notes]

3.2.6 Did all of the end user devices in your sample produce a warning or an opportunity to cancel before opening the email attachments containing executable (non-malware) files?

You should answer no if you were able to open an executable attachment without a warning or opportunity to cancel.

[Notes]

3.2.6.1 Has the client now addressed the configuration issue that allowed the executable to be opened without a warning or opportunity to cancel? Please provide notes on what happened.

[Notes]

3.2.7 For all devices in your sample using anti malware software that should defend against the test files, have you attempted to open both "executable" and "malware" test files using a web browser?

You must use a standard user account for this test (not an administrator account).

You must use the standard test files provided by IASME to carry out this test. You only need to send a subset of these files that would be appropriate to the device operating system (for example, Windows devices do not need to be sent the .dmg file, which is a macOS file). There are two types of test files - "malware" and "executable". Both types must be sent to every device in the sample. If in doubt, please verify your list of test files with IASME. You should send one email per file.

[Notes]

3.2.8 Were all of the downloads containing malware blocked by all of the end user devices in your sample?

If you identify a configuration issue, the client may be given an opportunity to address the issue and have a retest of a specific device carried out.

[Notes]

3.2.8.1 Has the client now addressed the configuration issue that allowed the malware to be opened? Please provide notes on what happened.

If you identify a configuration issue, the client may be given an opportunity to address the issue and have a retest of a specific device carried out.

[Notes]

3.2.9 Did all of the end user devices in your sample produce a warning or an opportunity to cancel before opening the downloads containing executable (non-malware) files?

If the browser prompts the user to decide whether to "run" or "save as" then this is classed as a pass for this test.

[Notes]

3.2.9.1 Has the client now addressed the configuration issue that allowed the executable to be opened without a warning or opportunity to cancel? Please provide notes on what happened.

If you identify a configuration issue, the client may be given an opportunity to address the issue and have a retest of a specific device carried out.

[Notes]

3.2.10 List the software that is installed on all devices and/or desktop environments that does not react to the test files.

Some anti-malware software does not use signature based scanning and so the EICAR files are not recognised as malicious.

This test must not be used for software that should be able to trigger the test files.

[Notes]

3.2.11 For all devices in your sample using anti malware software that does not trigger the test files, have you confirmed that the software is installed and operational through manual inspection of the logs on each device?

Some anti-malware software does not use signature based scanning and so the EICAR files are not recognised as malicious.

In these cases a manual check of the logs must be carried out on each device and/or desktop environment that uses this software to confirm that the software is operational.

[Notes]

3.2.11.1 Has the client now addressed the configuration issue that caused the software to not be operational.

Please provide notes on what happened.

If you identify a configuration issue, the client may be given an opportunity to address the issue and have a retest of a specific device carried out.

[Notes]

3.2.12 For all devices in your sample using anti malware software, have you confirmed that the software has been updated in accordance with the vendor's configuration instructions?

[Notes]

3.2.12.1 Has the client now addressed the configuration issue that caused the software to not be up to date? Please provide notes on what happened.

If you identify a configuration issue, the client may be given an opportunity to address the issue and have a retest of a specific device carried out.

[Notes]

3.2.13 Please provide information about the remediations carried out including the date that they were retested.

[Notes]

Malware Protection Using Certificate Based Application Allow Listing

3.3.1 For all devices in the sample relying on B - certificate based application allow listing, have you confirmed that the list of trusted root certificates are provided by the operating system manufacturer?

[Notes]

3.3.2 Have the additional certificates been added with the client's explicit agreement?

Root certificates that are not from the operating system are allowed if the client is aware that they are there and the purpose of them.

Additional certificates could be in place for reasons such as mobile device management.

[Notes]

3.3.2.1 Has the client now removed the unknown root certificates? Please provide notes on what happened.

If you identify a configuration issue, the client may be given an opportunity to address the issue and have a retest of a specific device carried out.

[Notes]

3.3.3 For all devices in the sample relying on B - certificate-based application allow listing, has it been confirmed that an unsigned executable and executables with a certificate that does not chain to a trusted certificate will not run on the end user device?

[Notes]

3.3.3.1 Has the client now addressed the configuration issue that allowed the executable to run on the device? Please provide notes on what happened.

If you identify a configuration issue, the client may be given an opportunity to address the issue and have a retest of a specific device carried out.

[Notes]

3.3.4 For all devices in the sample relying on B - certificate-based application allow listing, have you confirmed that operating system policy settings are in place to ensure that code signing applies to all of the applicable file formats to the relevant device?

[Notes]

3.3.4.1 Has the client now addressed the configuration issue that prevented code signing from applying to all applicable file formats for the device(s)? Please provide notes on what happened.

If you identify a configuration issue, the client may be given an opportunity to address the issue and have a retest of a specific device carried out.

[Notes]

3.3.5 Are you satisfied that every device in your sample is protected from malware using one of the methods described in Q3.1.2? If NO, please add notes to explain why.

[Notes]

3.3.6 Please provide information about the remediations carried out including the date that they were retested.

[Notes]

Review of Multi Factor Authentication Configuration

To test that cloud services declared in scope have been configured for multi-factor authentication (MFA).

Users of sampled devices to attempt to log into the organisations cloud services using their organisation issued accounts.

All cloud services to be tested for User and Administrator Access. Where multiple cloud services share an authentication service this test only needs to be performed once for each authentication service.

4.1.1 Provide a list of all cloud services used by the applicant that provides an authentication service.

A list of all cloud services tested must be provided.
Any cloud service that has been declared in the verified self assessment as not providing MFA does not need to be tested.
Where a cloud service authenticates through another cloud service, only the authentication service needs to be tested in the sample. (For example if an organisation authenticates 10 x cloud services via Azure SSO, only the Azure would need to be tested).

[Notes]

4.1.2 Were all users challenged with an MFA prompt prior to a successful login using an incognito browser or untrusted device?

Notes required *- result must be recorded for each cloud service tested.*

Observe the users trying to log in with their standard user accounts to each cloud service that they use.

This test is carried out against the user accounts belonging to the user that would use each sampled device to carry out their daily tasks. If the user is also an administrator for that service, ask them to login with their administrator account using the same method.

Answer No if an MFA prompt wasn't provided and the user successfully logged into the cloud service.

[Notes]

4.1.2.1 Has the client now addressed the configuration issue and enabled MFA on the service?

Notes required *-result must be recorded for each cloud service tested which failed the MFA checks.*

When cloud services that have MFA but it has not been configured have been identified the client must remediate and be retested by the CE+ assessor within the 30 day remediation window.

[Notes]

4.1.3 Have all cloud services as listed in the verified self-assessment been checked to confirm that MFA has been applied?

All cloud services listed in the verified self-assessment that have not been declared as 'not providing MFA in A7.15' must have their authentication method checked.

All authentication methods must have been checked with one Administrator and one standard user. If any of the cloud services were not checked as part of the sample an additional administrator and / or user must be checked.

Where an organisation does not have any standard users, please provide notes to detail this.

[Notes]

4.1.4 Please provide information about the remediations carried out including the date that they were retested.

[Notes]

Confirmation of Account Separation

Perform this test on any sampled end user device, servers that provide a user-interactive desktop and cloud environments where administrative processes can run.

The purpose is to test that user accounts don't have administrator privileges assigned.

5.1.1 Has every user account on the sampled devices confirmed to you they are logged in with a Standard User account?

This test is carried out on all sampled end user devices and/or desktop environments with the account/s that the standard user/s that would normally use that device would use for their daily tasks.

You should check the name associated with each account to confirm the sample is true and representative.

[Notes]

5.1.1.1 Provide the quantity of accounts tested per sampled device.

[Notes]

5.1.2 For all end user devices and the accounts, when observing a standard user attempting to run a process, were they asked to enter administrator credentials?

If the user was not prompted for an additional login to a separate administrator account, answer No and describe what happened.

[Notes]

5.1.2.1 Has the client now addressed the configuration settings to ensure that account separation is in place and that a separate administrator account is required to carry out administrator tasks?

If the answer is No, please provide a summary of why the test has failed after remediation.

[Notes]

5.1.3 Please provide information about the remediations carried out including the date that they were retested.

[Notes]

Summary of findings

6.1.1 Provide a summary of your findings here – ideally one or two paragraphs to give a flavour of the report. Briefly mention locations and scope. You should also highlight any notable anomalies and action points, pointing the reader to the appropriate section of the report for more information.

[Notes]

6.1.2 A Lead Assessor must review and sign off the findings of this assessment and confirmed that they agree with them.

Please provide the name of the Lead Assessor for this assessment. If you are a Lead Assessor, please enter your own name (you will not require a second person to sign off the assessment).

A Lead Assessor is an assessor that holds one of the qualifications in List A of the Assessor Requirements document. A Lead Assessor must review and agree with the findings of any CE+ assessments issued by a CB. If the person carrying out the assessment is already a Lead Assessor, you will not require a second person to sign off the assessment.

[Notes]