

Cyber Essentials Plus Prerequisites And Success Criteria

Assessor expectations and pre-requisites

All Assessors are required to be appropriately trained and qualified to perform all aspects required to meet Cyber Essentials Plus certification.

The Assessor is expected to read and familiarise themselves with the associated Verified Self Assessment (VSA) before testing takes place. **When discrepancies have been identified the assessor should challenge the applicant organisation and remediate within the timelines outlined in the assessor guidance.** For example, if the scope for the CE+ is different to the one declared in the VSA.

The Assessor is required to have sufficient knowledge and experience of the tools used as part of the Cyber Essentials Plus audit processes. The Assessor should be able to provide sufficient information and guidance to technical members of the organisations IT department regarding any discovered vulnerabilities and suggested remediation.

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.

Success Criteria

For an organisation to successfully obtain Cyber Essentials Plus certification, they must meet the requirements for each element of testing. If an organisation fails any of the tests throughout the certification process, they would be awarded a fail overall.

- All external devices tested should have no vulnerabilities rated high risk or critical according to the CVSSv3 scoring mechanism (base scores).
- The organisation must pass the internal vulnerability assessment on all devices with no high or critical vulnerabilities present (for which a vulnerability fix is available) according to CVSSv3 (base scores).
- Any high or critical vulnerabilities, for both internal and external assessment, must be remediated and then rescanned before awarding a pass. If the organisation is unable to remediate a high or critical vulnerability, then a fail should be awarded for the particular test.
- Anti Malware protection should be checked to confirm that it is compliant. All Anti Malware Software, or Application Allow Listing methods must be configured correctly and the technical controls confirmed.
- The organisation must confirm that MFA is enabled on all Cloud Services.
- The organisation must confirm that account separation is configured. Standard users will need to confirm that they do not have the privileges to carry out Administrator tasks.