

Cyber Essentials Plus Timeline

CE Plus Timelines

The organisation being tested for CE+ must have already achieved the Cyber Essentials self assessment and the scope for the self-assessment must be the same as the scope for the CE+ test. CE+ assessments must be carried out **within three months of the organisation achieving Cyber Essentials self-assessment**. All CE+ audit data needs to be collated and stored by the certifying body for the lifetime of the certificate (12 months from the CE+ being issued).

Assessors can allow a maximum of 30 days from the initial CE+ assessment for a client to remediate an issue identified as long as it falls within the three month period. The Assessor must retest the specific issue/s identified and confirm it is resolved before issuing a certificate.

- If the client takes longer to remediate an issue, the whole CE assessment must be carried out again by the Assessor.
- If the client does not agree to remediate an issue identified in a CE+ assessment, the client must be awarded a fail overall.

Extensions will only be granted in exceptional circumstances. To apply for an extension, the Assessor must raise a support ticket with:

- Applicants name
- Date of Verified Self Assessment
- Date CE+ testing started
- Reason for the extension request
- Target date for completion

If an extension is required the Assessor must write the support ticket reference number in the relevant question in the CE+ report on the assessment portal.

CE+ Timeline Summary

90-Day Window:

- The CE+ process must be completed within 90 days from the date of the VSA.
- This timeline cannot be extended.
- Extensions to the 30-day remediation window within the 90-day timeframe will only be granted in exceptional circumstances

Sample 1 Testing and Remediation:

- After the first scan of Sample 1, there is a 30-day remediation window to address all identified vulnerabilities.
- All fixes for Sample 1 must be completed within this 30-day window.
- Remediations for Sample 1 must be applied to the entire scope declared in the self assessment, not just the sampled devices.
- A 72-hour (or 3 working days) notice period must be provided to the applicant before any testing or scanning of Sample 1.
- If the client refuses to remediate Sample 1, the VSA will remain in place, but CE+ certification cannot be awarded.

Sample 2 Testing:

- Sample 2 must also be scanned within the same 30-day remediation window as Sample 1.
- If Sample 2 contains vulnerabilities that were present in Sample 1, the CE+ certification cannot be passed, and the VSA will be revoked.
- A 72-hour (or 3 working days) notice period must also be provided to the applicant before any testing or scanning of Sample 2.
- If the client refuses to agree to Sample 2 being tested, the VSA will remain in place, but CE+ certification cannot be awarded.
- There is no remediation period for sample 2

Non-Compliance and Consequences:

- If Sample 1 is not remediated within the 30-day window and Sample 2 fails testing, the VSA will be rescinded.
- If the 90-day CE+ timeline expires without successful remediation of Sample 1 or if Sample 2 highlights unresolved issues, the entire CE process must be restarted.
- If it is determined at any stage that CE+ certification cannot be awarded, the applicant must restart **the entire** Cyber Essentials certification process, including initiating a new VSA and selecting new samples, if they need to achieve CE+.
- Important: Data from previous scans in a failed CE+ process must not be reused in the new engagement.

Key Deadlines:

- The 30-day remediation window for Sample 1 and the testing of Sample 2 must occur within the overall 90-day CE+ timeline.
- The 30-day remediation window cannot be extended beyond the final 90-day deadline.
- Resetting or extending the 30-day remediation window within the 90-day timeframe is strictly prohibited.