

Cyber Essentials Plus: Verification Tests and Data Retention Policy

The Cyber Essentials Plus certification process is designed to provide organisations with a high level of assurance regarding their cybersecurity measures. Certification Bodies and Assessors play a vital role in ensuring the integrity of the process, from conducting verification tests to securely retaining audit data.

Verification Tests

It is now required that the Assessor must verify the scope and segregation against the details provided in the Cyber Essentials self assessment. Before testing begins, the Assessor must have:

- obtained the appropriate written permission from the Applicant
- verified that the scope of the Cyber Essentials Plus assessment matches the scope described by the valid Cyber Essentials CE Verified Self-Assessment certificate
- verified by technical means that the scope of the Cyber Essentials Plus assessment matches the networks and systems being assessed
- verified by technical means that when the Cyber Essentials self-assessment scope is 'Partial', any sub-sets have been segregated effectively
- identified the samples to be tested, and when this testing will occur (see sample testing section)

i All evidence resulting from the verifications above is to be retained by the Certifying Body for at least the lifetime of the certificate.

The Assessor must verify that the sample size has been calculated correctly using the method described by the Delivery Partner. **Evidence of how the sample size was calculated must be retained by the Certifying Body for at least the lifetime of the certificate.**

Data Retention Policy

Certification Bodies are required to retain all audit data collected during the CE+ assessment for the lifetime of the certificate (12 months from the CE+ being issued). This policy ensures that the certification process is transparent and that evidence is available for quality assurance or investigations.