

# Danzell update - New CE+ internal vulnerability and remediation process

## Change in Remediation Process

The vulnerabilities identified in Sample 1 must be fixed across the entire scope of the CE Verified Self-Assessment certificate, not just the sampled devices. The second sample (Sample 2) is to verify that the remediation work has been carried out across the entire scope.

### Test of the First Sample (Sample 1)

The Assessor will test the random sample of devices chosen to confirm that all required updates have been applied. If all devices in the original sample are compliant, CE+ can be awarded. If any devices in the original sample are found to lack the required updates, the organisation fails the CE+ assessment at this stage.

### Remediation of Sample 1

If the organisation fails the test on Sample 1, they must remediate the issues identified in the original sample by applying the required updates. This must be completed within 30 days. Once remediation is complete, the Assessor will test Sample 1 again. If relevant updates are still missing after the 30 day remediation window, the organisation will fail the CE+ assessment, and the CE certificate will be revoked.

### Second Random Sample (Sample 2)

Where vulnerabilities have been found in devices tested in Sample 1, a second sample (Sample 2) should be taken. The purpose of this is to verify compliance with Security Update Management requirements which state that all high/critical updates must be applied within 14 days.

Sample 2 must use the same calculation used for Sample 1. When testing Sample 2, if any of the devices are found to contain the same vulnerabilities as in Sample 1, the organisation fails the CE+ assessment and the CE Verified Self-Assessment certificate will be revoked. If different vulnerabilities are identified in Sample 2, the organisation should be asked to address these. A re-test may be required depending on NCSC requirement.

**For Sample 2, the devices to be tested must be declared by the Assessor to the applicant not more than 72 hours or 3 working days prior to the second sample being tested. Sample 2 must be tested within the 30 day remediation window. There is no remediation window for Sample 2.**

Devices for Sample 2 must only be selected after testing of Sample 1.

- The Assessor will test Sample 2 devices to ensure that updates have been applied across the scope of the assessment.

- If the applicant refuses to allow testing of Sample 2 they cannot achieve CE+ However the

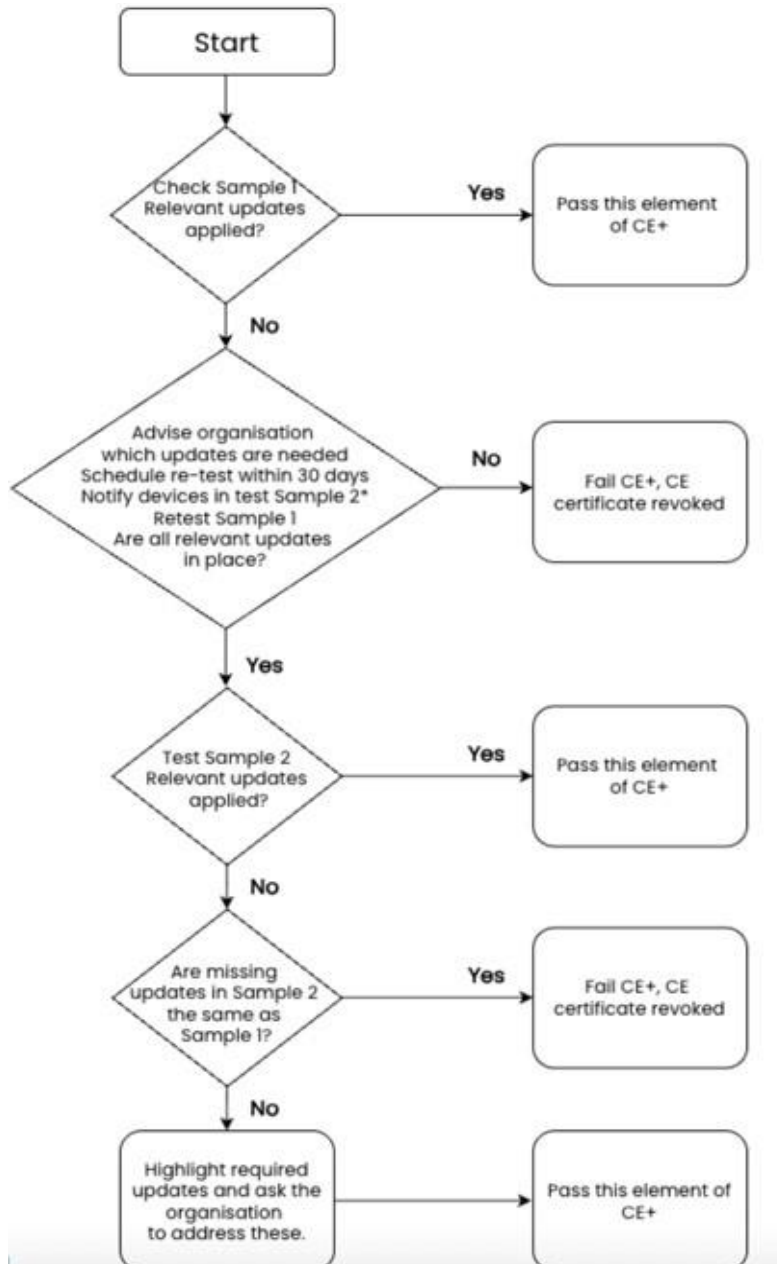
- If the applicant refuses to allow testing of Sample 2, they cannot achieve CE+. However, the CE Verified Self-Assessment certificate will remain valid.

## Outcome Based on the Second Sample

If all required updates are found to be installed on devices in Sample 2, the organisation will pass the CE+ assessment. If updates identified as missing in Sample 1 are also found to be missing in Sample 2, this indicates that remediation efforts were not applied throughout the scope. In this case, the organisation will fail the CE+ assessment, and their CE Verified Self Assessment certificate will be revoked.

If Sample 2 contains devices with missing updates that are unrelated to ones found in Sample 1, the organisation will pass the CE+ assessment but will receive an advisory to address these updates.

A flow diagram of the process can be seen below:



Any vulnerability found in Sample 2 that matches a vulnerability found in Sample 1 will lead to failure of the assessment.

## **Retesting Rules Summary**

If Sample 1 fails due to missing security updates, the assessor will retest the original sample and subsequently test a new random sample (Sample 2).

Any missing security updates in Sample 1 must be remediated across the whole scope of assessment. Sample 2 will be used to check that this has been done.

If Sample 2 fails due to missing security updates, and these missing updates are the same as in Sample 1, the CE+ assessment will fail and the CE Verified Self-Assessment certificate will be revoked.

### **For environments with restricted device counts, the following logic applies:**

**Retesting Sample 1:** The assessor will retest the Sample 1 devices that failed to confirm whether the missing updates have been applied. Any missing updates must be remediated.

**Exhausting the Pool:** If your total device count is small, the new sample should consist of any remaining devices in that were not part of the initial test.

**Total Coverage:** If all devices were already tested in the initial sample (for example, you only have 3 laptops and all 3 were tested), the assessor must verify the remediation by re-scanning the entire sample set to ensure no new vulnerabilities were introduced.

© The IASME Consortium Ltd 2026 All rights reserved.