



Cyber Essentials Plus Guide with Umbrella Cyber

You have **3 months** to complete Cyber Essentials Plus, from the date you certified to Cyber Essentials. This is a hard limit¹; so, we recommend that you aim to complete it within **10 weeks** at the most.

Full details of each step of this process are also provided on the first tab of the Cyber Essentials Plus tracker.

There are two stages to the assessment: vulnerability scanning and observational tests.

The first and **most important** steps are for you to provide a list of devices, IP addresses/host names & servers in the tracker and book in your assessment day/s. Without this we will not be able to proceed. We recommend the following steps are carried out in the next 1 to 4 weeks.

*Note, that, the only servers that we need to audit on a meeting are those which provide users with a remote desktop environment (e.g., RDS or Citrix servers). Please let us know if any of your servers provide such services. All other Servers will be sampled for vulnerability scanning.

Weeks 1 - 4:

- Provide a full list of all devices (computers, mobile devices, servers) and the IP addresses of any internet-facing devices (e.g, routers/firewalls) in the tracker.
- Book the assessment day/s with your assessor.
- We will then select a random set of users from the tracker whose devices we will assess.
- Once you have confirmed those users are available on the assessment day/s we will send them calendar invites to their assessment slot which should take no more than 30 minutes each.
-

Weeks 4 - 10:

Vulnerability Scanning:

Once we have selected the sample of users we will be assessing we will send you details of how to install our vulnerability scanning software on their computers. This will need to be **installed as soon**

¹ Failure to complete the process within this time scale will require you to re-certify to Cyber Essentials to continue with Cyber Essentials Plus



as possible, so that we can begin the scanning. These scans run in the background and do not interrupt their work routine.

*Please note we will run a scan to ensure we have captured all the devices. We will then run a report to highlight any concerns or areas for remediation. We will then run further scans and remediation reports until all scans are compliant.

Observational tests:

For the observational tests carried out on the assessment day, each user will need to be present to share their screen with us and follow some simple instructions allowing us to view the compliance of the devices in line with the Cyber Essentials standard. These tests are detailed below:

- We check that users are logged in using a standard account and are not logged in as administrator. We also check that two-factor authentication is in place for accessing cloud services.
- A series of test emails with attachments which mimic malware will be sent to users to observe how their email clients process them.
- We also check how the computer's internet browsers process similar malware/executable files delivered via test-malware site which we host.
- For mobile devices we will use remote sharing to establish whether the device is jailbroken/rooted, the operating system version is compliant, and whether there are any unknown profiles installed.

As there are multiple stages to the Cyber Essentials Plus assessment, we will work closely with you to ensure we are keeping on track to reach certification well within the 3-month timeframe. The key to the process running smoothly is to **fill in the tracker as soon as possible** and to **book in your assessment date**.

We look forward to working with you!