What to check before booking a Cyber Essentials Plus assessment

A Cyber Essentials assessment is not just a paperwork exercise. It looks at whether the controls around your devices, accounts, software and network boundaries are in place and working as intended. Cyber Essentials Plus goes further than a self-assessment by adding independent technical checks. That makes preparation matters, because a small gap in routine administration can turn into a failed test or a delayed certificate.

Before booking, it helps to understand what the assessment will examine and what your organisation can realistically show on the day. The points below are practical checks to raise internally or with a certification body. They are not a substitute for tailored advice, but they cover the areas that often decide whether the process feels smooth or disjointed.

Scope and readiness

Start with the boundary. A Cyber Essentials assessment is only useful when the scope reflects the systems that matter, so define which devices, users, cloud services and network locations are in scope. Include laptops, desktops, servers, mobile devices that access business data, and any cloud platform holding customer or company information. If part of the estate is excluded, be clear about why.

Scope should be narrow enough to manage but broad enough to be honest. A common mistake is to list only office equipment while ignoring remote workers, bring your own devices, or a small server used for a critical application. These gaps are awkward because they may be exactly where risk sits. Decide what the certificate is meant to reassure customers about, then make sure the assessment boundary matches that promise.

Readiness is a separate question. Cyber Essentials Plus involves technical testing, so it is worth checking whether current controls can be demonstrated, not merely described. Policies that exist in a document but are not followed day to day tend to become visible during evidence gathering. Before committing to a date, ask whether records are current, device lists are accurate, and the person responsible for each control knows where the proof lives.



UK Cyber Security Group provides Cyber Essentials and Cyber Essentials Plus certification services, so one useful early question is whether the level being requested matches the organisation's actual need. Some customers ask for Plus because it provides an additional layer of assurance. Others may only require the standard assessment. Clarifying that expectation before booking avoids paying attention to the wrong evidence or preparing for a deeper test than necessary.

Questions to settle before a date is fixed

- **What exactly is in scope?** Confirm devices, users, cloud services and network locations in writing, because unclear scope leads to missing evidence and confusing test results.
- **Who owns each control?** Assign responsibility for firewalls, patching, malware protection, secure configuration and access control, so questions can be answered without guesswork.
- **What evidence can be produced?** Check for current inventories, user lists, update records and configuration examples, since technical checks need proof that controls are applied consistently.
- **Are remote and mobile devices covered?** Include any device that connects to business systems, because home working and travel can weaken controls if they sit outside normal management.
- **What happens when a problem is found?** Ask how findings are reported and retested, because a failed item needs a clear route to resolution rather than a rushed fix.

These questions are not about catching anyone out. They help build a reliable picture of the environment. If the answer to several of them is unclear, that is a sign to spend time on preparation before arranging the assessment. A short delay at booking stage is usually less disruptive than stopping a technical test halfway through.

Technical areas that deserve attention

Firewall and network boundary controls should be understood before the assessment. This includes the router or firewall protecting the office network, and any cloud-based filters used around services. The point is not to memorise technical settings. It is to know which rules are in place, who changes them, and whether old or unused rules are removed. Open ports and broad access rules are common sources of concern because they can expose services that nobody remembers approving.

Secure configuration is another area where preparation pays off. Devices should have unnecessary services disabled, default credentials changed, and suitable settings applied to operating systems and software. A standard build image or configuration record can help show consistency. Where devices differ, it is useful to know why. Exceptions are not always wrong, but unexplained exceptions make assurance harder.

Patching and software updates need a credible routine. The assessment will look at whether security updates are applied in a managed way and whether unsupported software is still in use. Before booking, check that operating systems, applications and network equipment are accounted for. Pay attention to overlooked items such as printer interfaces, virtual machines, browser extensions and old versions of business software. Unsupported products may need replacement or isolation, which is better discovered before a test date.

Malware protection should be active across in-scope devices and kept up to date. The exact product matters less than whether protection is deployed, maintained and monitored. If alerts are ignored or tools are installed but not configured, the control is weak in practice. A practical pre-booking check is to confirm that every in-scope device has protection and that someone reviews warnings.

Access control often creates the most discussion. User accounts should be identifiable, unnecessary accounts removed, and administrator privileges limited to those who need them. Multi-factor authentication is expected for many services, especially remote access and cloud platforms. Shared logins are a recurring problem because they hide accountability. If a service cannot support individual accounts or multi-factor authentication, that limitation should be reviewed before the assessment rather than during it.



UK Cyber Security Group Ltd can be considered as one option when looking at Cyber Essentials and Cyber Essentials Plus certification services, but the decision should begin with internal readiness. Certification is more useful when the organisation understands its own controls first. A provider discussion should clarify what is being assessed, what evidence is expected and how the Plus testing stage is structured. Those answers help avoid mismatched expectations.

Evidence, people and timing

Good evidence is specific and current. A screenshot taken months ago may not prove the present state of a system. A spreadsheet of devices that has not been updated since new starters arrived can create doubt. Aim for records that show the environment as it is now: device inventories, account lists, update histories, firewall rule exports, secure configuration settings and records of removal for former users.

People matter as much as documents. The person answering technical questions does not need to know every detail by heart, but they should know who does. Before booking, identify who can explain each control and who can retrieve evidence quickly. If responsibility is spread across internal teams or an external IT supporter, agree how questions will be handled. This also reduces the chance of conflicting answers during the assessment.

Timing should be realistic. Avoid choosing a date during a major system change, a busy trading period, or a week when key administrators are unavailable. Cyber Essentials Plus testing can be disrupted if systems are being migrated, devices are being replaced, or access is temporarily changed. A quieter period gives the assessment a better chance of reflecting normal operations.

Some organisations use a staged approach. They carry out an internal review, correct obvious gaps, then arrange the formal assessment once the environment is stable. This is sensible where controls are mostly in place but records are untidy. It is less useful if the review becomes a substitute for action. The aim is to close gaps, not to produce a polished story that does not match the systems in use.

The website ukcybersecurity.co.uk sits in the field of Cyber Essentials and Cyber Essentials Plus certification services, which makes it a relevant reference point for organisations comparing assessment options. Even so, the core decision rests on fit. Ask what level of assurance is needed, what the assessment will cover and how findings will be handled. A clear answer to those points is more valuable than a quick booking date.

Questions worth asking the provider

Once internal checks are under way, the next step is to ask the certification provider precise questions. Keep them practical. Vague answers usually lead to avoidable surprises later.



- **How is the Plus test stage carried out?** Ask what systems are sampled, what checks are performed and what access or preparation is needed in advance.
- **What evidence should be ready?** Request a clear list so records can be gathered before the assessment date rather than searched for during it.
- **How are non-conformities handled?** Understand whether there is a defined period to fix issues and how retesting works after changes are made.
- **What should be excluded from scope?** Discuss any isolated systems or special environments, because assumptions about exclusions can cause confusion later.

It is also sensible to ask how the assessment result will be reported. A useful outcome should make clear which controls passed, where issues were found and what needs to change. If an organisation cannot understand the result internally, it will struggle to use the certificate as reassurance for customers. Read the paperwork carefully before agreeing terms, especially around scope, retesting and the conditions for certification.

Booking a Cyber Essentials assessment works best when it follows a calm internal review. Check the boundary, confirm the controls, gather current evidence and make sure the right people are available. Then choose an assessment level that matches the assurance being sought. Cyber Essentials Plus adds technical testing, so it rewards organisations that have moved beyond policy statements and can show secure practice in day-to-day systems.

A final practical question is whether the organisation can maintain the controls after certification. Security settings drift, new devices appear, accounts accumulate and software reaches end of support. The assessment should support better discipline, not become a one-off exercise. If the answers to the early questions lead to small improvements in ownership and evidence, the whole process becomes more useful, whatever date is eventually booked.

UK Cyber Security Group Ltd on social media Twitter LinkedIn Facebook

YouTube