What multi-office organisations should check for Cyber Essentials compliance

Multi-office organisations often find that Cyber Essentials compliance is less about one perfect document and more about consistent controls across every place where people work. A head office, a small satellite team, a warehouse terminal and a remote worker's laptop may all fall within scope. The aim is to show that security basics are applied in a repeatable way, not left to each office to interpret.

The scope needs to be settled before the finer points are reviewed. If one site is included and another is left out without a clear reason, evidence becomes patchy and answers vary from team to team. A useful starting point is to list the offices, the systems they use, the devices that connect to company data and the people who can approve access.

Define the boundary across every office

Start by agreeing which systems, devices and users sit inside the certification boundary. In practice, that means looking at laptops, desktops, servers, cloud services, network equipment and mobile devices used for work. Shared platforms matter too, especially where one office uses a local tool that others never touch.

Write the boundary in plain language. Instead of saying that all office systems are included, name the domains, cloud tenancies, device groups and locations. This helps when evidence is requested later, because each answer can be tied to a defined area. It also reveals weak spots, such as a branch that still uses a personal email account for work documents or a shared login that nobody owns.

Where offices differ, record why. A site with only tablets and a browser-based system may have a different control set from a site with local servers. The controls still need to protect in-scope systems, but the evidence can reflect the way each site works.

Inventories need to match reality

An asset list that was accurate at the time it was written can drift quickly. New starters receive laptops, old devices move between offices, and cloud subscriptions appear when a team solves a local problem. Before pursuing UK Cyber Security Group Ltd Cyber Essentials Plus quote, make sure the inventory reflects the estate as it operates now, not as it was imagined.

- **Devices:** check each office for work laptops, desktops, phones, tablets and network hardware, including spares and loan devices that sit in drawers.
- **Users and access:** compare current staff lists with active accounts, shared mailboxes and administrator roles, then remove access that no longer has a clear owner.
- **Software and cloud services:** record the tools used to store, send or process business data, including services bought by a local team.
- **Support arrangements:** note who maintains each site's equipment and how security updates reach devices that are not in the main office.
- **Physical locations:** keep a simple site list so each office can be linked to its devices, network and responsible manager.

The reason for this detail is straightforward. Cyber Essentials compliance depends on protecting in-scope systems, and protection is hard to demonstrate when nobody can say what those systems are. A short, current inventory is more useful than a long document full of old entries.

Check access control at a practical level

Access controls should be understandable by the people who use them every day. Review account types across all offices, focusing on administrator privileges, shared accounts and former staff access. Administrator rights should be limited to people who need them for work, and separate accounts should be used where daily work does not require elevated access.

Passwords are another area where multi-site consistency matters. Look for reusable passwords, passwords written on desks and accounts protected only by a weak phrase. Multi-factor authentication should be applied wherever it is available, especially for remote access, cloud email and administrative portals. If an office relies on a shared device, make sure individual accounts are still used, so actions can be attributed to a person.

Leaver processes deserve close attention. A person who moves from one office to another may keep old permissions long after the change. Build a simple handoff between HR, line managers and whoever manages access, so role changes remove rights that are no longer needed.

Keep patching and malware protection current

Patch management across several offices needs visibility. A central device list helps, but local knowledge often reveals machines that rarely connect to the main network. Check that operating systems, browsers and common applications receive updates, and that devices can obtain those updates without someone manually remembering every month.

Malware protection should be active on supported devices and kept up to date. Look beyond the presence of an icon on a screen. Confirm that protection is enabled, definitions are current and alerts reach someone who can act. Where a site uses a specialist system that cannot run standard software, record the compensating controls and seek advice on whether it belongs within scope.

Supporting evidence works best when it is routine. Export reports from management tools, keep dated records of update activity and retain examples of how exceptions are handled. This avoids a last-minute search through inboxes when certification evidence is needed.

Review firewalls, networks and secure configuration

Network boundaries vary between offices. One site may have a managed firewall, another may rely on a router provided by the internet supplier, and a smaller team may work through cloud services only. Each arrangement should be checked against the way data flows in and out of the organisation.

Default settings are a common source of risk. Change default passwords on network equipment, close unused remote access routes and remove services that are not needed. Keep firewall rules documented in plain terms, including why each rule exists. Rules that nobody can explain tend to linger long after the original need has gone.

Secure configuration also covers everyday devices. Disable unused accounts, remove unnecessary software and avoid local administrator rights for general users. Build a standard setup for new laptops so each office starts from the same baseline. Where local needs require changes, note the reason and keep the deviation small.

Prove that controls work, not just that they exist

Certification evidence should show operation over time. Policies alone do not demonstrate that access is reviewed, updates are applied or insecure settings are corrected. Keep records that a reviewer can follow without needing a long explanation from each office manager.

Useful evidence tends to be simple: a user list with approval dates, a device report showing update status, a configuration standard with a few completed examples, and a record of how exceptions were handled. When the same process is used in several offices, sample records from more than one location. That helps show that the approach is consistent rather than limited to the main site.

UK Cyber Security Group Ltd provides Cyber Essentials and Cyber Essentials Plus certification services to help organisations protect systems, demonstrate effective security controls and reassure customers. That context makes preparation more than an administrative exercise. The evidence should reflect controls that staff recognise and can describe, whether they work in a large office or a small satellite team.

Give each office a clear owner

A multi-office programme needs named responsibility at each location. This does not mean every office manager becomes a security specialist. It means someone checks that devices are reported, access changes are raised and questions can be answered with real examples. A central lead then pulls the information together and resolves gaps.

Regular reviews help keep the programme steady. Short, scheduled checks of accounts, devices, updates and network settings are easier than a rushed annual exercise. The exact rhythm can depend on the size of each site, but the record should show that reviews happen and that findings are closed.

Preparation works best when the same language is used everywhere. People should know what counts as an in-scope device, who can grant access and where to report a lost laptop or a

suspicious message. Clear ownership turns Cyber Essentials compliance from a document exercise into a set of habits that survive staff changes, office moves and new tools.

UK Cyber Security Group Ltd on social media Twitter LinkedIn Facebook

YouTube