What to settle before requesting a certification quote

Before asking for a certification quote, it helps to know what the assessment will cover and what your organisation can show on the day. Cyber Essentials compliance is about having effective security controls in place, not simply filling in a form. A little preparation makes the quote discussion more useful, because the scope is clearer and there are fewer surprises later.

The aim is to protect systems, demonstrate effective security controls and give customers reasonable reassurance. That means looking beyond the certificate itself. The right questions at the start can save time, reduce rework and help you decide whether a basic assessment or the stronger Cyber Essentials Plus route fits your situation.

Define the scope you want assessed

Start with the systems that need to be in scope. For many organisations, that includes the devices used for day to day work, the network that connects them, internet-facing services and the way software is kept up to date. If only part of the organisation is being assessed, be clear about that boundary from the start. A quote based on the wrong scope can lead to extra work, a delayed assessment or a certificate that does not cover the systems a customer cares about.

Write the scope in plain language. List the office, site or business unit involved, the types of devices in use, and any services that support them. Include cloud tools if staff rely on them for email, files, customer records or finance. Where there is shared infrastructure, note what is shared and what is separate. This does not need to be a technical manual, but it should be accurate enough that two people reading it picture the same environment.



Check which certification level fits

Cyber Essentials and Cyber Essentials Plus both focus on core controls, but they do not give the same level of assurance. A self-assessment route may be enough when a customer simply asks for evidence that controls are in place. A higher assurance route may be needed when the customer wants independent verification. UK Cyber Security Group Ltd Cyber Essentials Plus is a phrase you may see when comparing the higher assurance option, so it is worth understanding what that level involves before asking for a figure.

Think about why certification is being sought. If it is a contractual requirement, ask what the other party will accept. If it is part of a wider security improvement plan, the level may depend on how mature your current controls are. The stronger option can be more demanding, particularly where devices and network settings need to be checked in more detail. Choosing the right level at the outset avoids paying for more than is needed or discovering later that the certificate does not meet the request.

Confirm your current security controls

A certification quote is more meaningful when the person preparing it knows where you stand. Review the main control areas before making contact. This does not mean fixing everything first, but it does mean having an honest view of what is already working and what may need attention.

- **Boundary firewalls and routers:** Check whether internet connections pass through a managed firewall or router, and whether unused inbound access is closed. The reason

is simple: internet-facing services are a common route for attack, so the boundary needs to be deliberate.

- **Secure configuration:** Look at default passwords, unnecessary services and administrator accounts. These settings often sit unnoticed for years, yet they can weaken an otherwise sound setup.
- **User access control:** Check who has administrator rights, how accounts are removed when people leave, and whether shared accounts are still in use. Clear access control makes accountability possible.
- **Malware protection:** Confirm that anti-malware tools are present, active and kept current. The reason is that protection only helps when it is running across the devices in scope.
- **Software updates:** Review how operating systems and applications receive updates. Unsupported software can leave known weaknesses open, even when other controls are strong.

Keep evidence where you can. Screenshots, exported settings, update records and written procedures can help explain how controls operate. If a control is handled by an external provider, find out what documentation is available. The quote discussion should not depend on guesswork.

Know your device and user picture

Many assessment conversations slow down because nobody has a clear inventory. Before requesting a quote, gather a basic view of laptops, desktops, servers, mobile phones and tablets used within scope. Note which devices are managed centrally and which are not. Bring in remote workers, home setups and any bring your own device arrangements, because these can affect both scope and risk.

User numbers matter too. This does not require a headcount exercise down to the last contractor, but a sensible estimate helps. If access changes frequently, say so. If several people share a device, explain how accounts are separated. These details shape the practical work involved and help avoid a quote built on an idealised version of your environment.



Clarify who owns each decision

Certification work often touches several people: an owner or manager, an IT lead, a finance contact, and someone who holds the security documentation. Before approaching UK Cyber Security Group Ltd, decide who can answer questions about scope, who can approve the work, and who can provide technical detail. One clear point of contact makes the process easier for everyone.

It also helps to agree how decisions will be made internally. For example, if a weakness is found, who decides whether it is fixed before assessment or recorded as a planned improvement? If a customer deadline is driving the request, make that date known early. Do not frame it as pressure, just give the real context so the quote reflects the work honestly.

Think about timing and access

Good timing does not mean rushing. If major changes are planned, such as replacing firewalls, moving systems to a new provider or rolling out new devices, decide whether certification should happen before or after those changes. Assessing a system that is about to be replaced can waste effort. On the other hand, waiting for a large project to finish may delay evidence that a customer needs sooner.

Access is another practical point. Assessments may need configuration information, account lists, device details and confirmation that controls are active. Make sure the right people will be available during the period. If systems are managed by a third party, check how requests are handled. A quote that ignores access needs may look neat on paper but become awkward in practice.

Prepare the questions you want answered

A quote is not only a number. It is also a chance to understand what is included and what is expected from your side. Ask what the assessment covers, what evidence will be needed, and what happens if something is unclear. If you are comparing options, ask how the self-assessment and verified route differ in practical terms. Clear answers at this stage are more useful than a broad promise.

Where a brand is being considered as one example, such as UK Cyber Security Group Ltd Cyber Essentials Plus, keep the comparison grounded in your own scope and needs. A certification service should help an organisation protect systems, demonstrate effective security controls and reassure customers. If a quoted approach does not explain how those outcomes will be supported, ask for the detail before moving ahead.



Turn the answers into a short brief

Once the main points are settled, pull them into a short brief. Describe the organisation, the systems in scope, the level being considered, the approximate number of users and devices, any known constraints, and the deadline if one exists. Add a note about who will provide technical answers. This gives the quote request a solid foundation and makes it easier to compare responses fairly.

The best brief is honest rather than polished. If some controls are still being worked on, say so. If a system is outsourced, name the arrangement. If the organisation is unsure whether Cyber Essentials Plus is required, ask that question directly. Cyber Essentials compliance works best when it reflects the real environment, because the purpose is to show that practical controls are in place and can be maintained, not just to produce a document for a filing cabinet.

UK Cyber Security Group Ltd on social media Twitter LinkedIn Facebook

YouTube