Cyber Essentials preparation checklist_

Understand the core controls

First, you need to understand the core controls Cyber Essentials is based upon and how to build them into your business. Here's our top tips for implementing the core controls.

Click to tick ✓

Firewall assessment	
Firewalls: Ensure that software firewalls are enabled on all endpoints / workstations accessing your organisation and use a boundary firewall at each of your business premises (managed offices do not require this). A hardware firewall is a dedicated physical device (ideal for network protection if your staff are based at one location), while a software firewall is a program running on a computer (these help secure remote workers' devices).	☐
Firewall configuration: Ensure firewalls are configured to block unnecessary inbound ports and services.	☐
Firewall configuration reviews: Firewall rules and policies should be regularly reviewed to ensure only those still required by your organisation are active and open, with justification recorded.	☐

Secure configuration	
Secure default configurations: Ensure devices and software are configured with secure default settings, which should align with security best practice and your internal policy. Look to change default passwords on new devices (including firewalls), uninstall unnecessary included software, disable auto-run features and disable any users accounts and services not needed.	☐
Secure access to devices and services: Users should need to authenticate to access a computer or cloud service, so things like automatic screen locking should be used.	☐
Device-unlocking controls: You should also require a minimum of a 6-digit PIN for unlocking a phone or computer where the user is present.	☐

Malware protection

Anti-malware software: Use antimalware software to protect against other types of malicious software, again like Microsoft Defender.	☐
Automatic scans: The anti-virus solution should automatically perform scans for malware and other threats when files are programs are opened.	☐
Web filtering: Browsing the internet should be protected by scanning web pages automatically and prevent connections to known malicious websites.	☐
Approved applications: Maintain a list of approved applications and ensure users abide to this. You can make use of official app stores and application signing for mobile devices. This can be an alternative to anti-malware software.	☐

Patch management

Licensed and supported software: All software you use must be actively supported by the supplier, even if not the latest version. Where software is out of support it must be removed, upgraded or segregated from the rest of your network.	☐
Software updates: Keep all software, including applications and firewall firmware, up to date. This also applies to third party applications. Critical security patches must be applied within 14 days of release.	☐
Operating system patches: Implement a regular patching schedule for all operating systems. Many system providers will remind you ahead of patch updates.	☐
Automated patching: Where possible, use automated tools to deploy patches efficiently.	☐

User access control

Approval process: Have a user account creation and approval process for consistency across new users.	☐
Strong password policies: Enforce best practice password/PIN policies, including encouraging unique passwords, delivering staff awareness training and granting self-service password reset abilities.	☐
Least privilege principle: Grant users only the minimum level of access required to perform their job duties.	☐
Administrative separation: All administrative activities must be performed by separate user accounts from your day-to-day login that access the internet and email.	☐
Account management: Regularly review and disable inactive user accounts.	☐
User access controls: Implement strong access controls, including multi-factor authentication (MFA) for all cloud services where possible. This includes Microsoft 365.	☐

Document your security practices

Once you've implemented these security practices, you'll want to document them to help with auditing and create a consistent policy to follow.

- [ ] **Inventory hardware and software:** Create a detailed inventory of all devices, software and cloud services.
- [ ] **Document security policies:** Develop clear policies and procedures for password management, firewall management, user access control and incident response.
- [ ] **Record configuration changes:** Keep a record of any changes made to system configurations.

Choose a certification body

Your certification body will provide the assessment and your certificate, so choose wisely.

- [ ] **Research certification bodies:** Identify accredited certification bodies like IASME or IT Governance.
- [ ] **Select a certification body:** Choose a certification body that suits your needs and budget.

Prepare for the self-assessment

Next, you need to prepare to pass the self-assessment questionnaire. Your certification body will provide this.

- [ ] **Gather information:** Collect all necessary documentation, including policies, procedures and configuration settings.
- [ ] **Complete the self-assessment questionnaire:** Answer the questions accurately and honestly.
- [ ] **Review and verify:** Double-check your answers to ensure accuracy.

Submit the self-assessment

Now, it's time to submit once you're happy with your questionnaire answers.

- [ ] **Submit to certification body:** Submit your completed self-assessment to the chosen certification body.
- [ ] **Pay the fees:** Pay the required fees for the certification process.

OPTIONAL/NICE TO HAVE

Technical validation (for Cyber Essentials Plus)

This is an additional step you'll need to undertake to get Cyber Essentials Plus, if that's your chosen route.

Vulnerability scanning: Conduct vulnerability scans to identify potential weaknesses.	☐
Penetration testing: Simulate cyber-attacks to test your defences.	☐
On-site assessments: Prepare for potential on-site assessments by the certification body.	☐

Certification

Review and verification: The certification body will review your self-assessment and technical validation (if applicable).	☐
Certification award: Upon successful review, you will receive your Cyber Essentials or Cyber Essentials Plus certification.	☐

How can Infinity Group help with Cyber Essentials?

We've worked with many clients to undertake their Cyber Essentials audits. Our affordable Cyber Essentials certification packages include:

- **An on-site audit of your current setup (typically taking 4 hours)**
- **A list of recommendations in line with Cyber Essentials' strict certification criteria**

Our specialist IT security team in-house that can easily undertake the tasks outlined in the audit quickly to ensure our clients pass the certification as quickly as possible.

In the case of Cyber Essentials Plus, we can also arrange for you to undertake an assessment for this once you have received Cyber Essentials certification and support you in meeting the criteria required for this.

Get in touch to find out more.

hello@infinitygroup.co.uk
0330 191 1701
infinitygroup.co.uk