



CYPHERE

● FREE CHECKLIST

# Cyber Essentials and Cyber Essentials Plus readiness checklist

A printable checklist for both certification levels, organised by the five NCSC controls and updated for the Danzell question set (v3.3), which applies to every new assessment from 27 April 2026.

thecyphere.com | info@thecyphere.com | +44 (0) 333 050 9002

## How to use this checklist (Danzell question set, v3.3)

- ✓ Sections 0 to 5 apply to Cyber Essentials. The audit preparation list applies if you go on to Plus, which must be completed within 90 days of your basic certificate.
- ✓ Work through it before you open the question set, not while you answer it; contradictory answers are a common reason submissions come back.
- ✓ Tick an item only when you can show evidence for it; those records are the ones an assessor asks for.
- ✓ Clear the three automatic fails first: unsupported software, cloud services without MFA, and critical or high updates not applied within 14 days.

## FREE OFFICIAL RESOURCES

### Preview the question set

IASME publishes the self-assessment questions free. Read them first.

### Readiness tool

Answer questions about your setup and get an action plan back.

### Knowledge Hub

IASME's guidance on each control, with worked examples.



HM Government  
**G-Cloud**  
Supplier



IASME  
CYBER  
ASSURANCE



30+ five-star  
Google reviews



# Scope, firewalls and secure configuration

## 0 Scope and inventory

- ☐ Scope agreed in writing with your certification body: the whole organisation, or a sub-set separated by a firewall or VLAN
- ☐ Asset list of every in-scope device (desktops, laptops, thin clients, virtual desktops, servers, phones, tablets, firewalls, routers) with operating system and version
- ☐ Every cloud service holding your data is listed (email, file storage, CRM, finance, HR, collaboration tools); none can be left out of scope
- ☐ For each cloud service you know which controls the provider runs and which you configure; a SaaS service still has to be set up securely by you
- ☐ Personal devices that access work email or data are listed, whether they belong to staff, volunteers or trustees (a phone used only for calls, texts and MFA apps is out of scope)
- ☐ Every in-scope legal entity is listed with its name, address and company number

## 1 Firewalls

- ☐ No internet access to the firewall administrative interface; where there is a documented business need, it is protected by MFA, or by an IP allow list and a strong password
- ☐ Default administrative passwords changed to strong, unique passwords, or remote administration disabled entirely
- ☐ Unauthenticated inbound connections blocked by default (for cloud services, through data flow policies)
- ☐ Every inbound rule approved and documented by an authorised person, with the business need recorded
- ☐ Rules reviewed regularly and outdated or unnecessary rules removed
- ☐ Software firewall switched on for devices used on networks you do not control (home broadband, public Wi-Fi); a router you supply to a home worker is in scope, other home routers are out

## 2 Secure configuration

- ☐ All default and guessable passwords changed
- ☐ Unnecessary software, services and accounts removed or disabled (guest accounts, unused admin accounts)
- ☐ Auto-run disabled so nothing executes without user authorisation
- ☐ Device unlock in place on every user device: biometric, PIN or password (a PIN used only to unlock is at least 6 characters; where it is also the login credential, the full password rules apply)
- ☐ Brute-force protection: no more than 10 guesses in 5 minutes, or lockout after no more than 10 failed attempts
- ☐ Password quality enforced by technical controls: MFA with a password of at least 8 characters, or a minimum of 12 characters, or a minimum of 8 characters with common passwords blocked
- ☐ Password expiry and forced complexity rules switched off; the NCSC advises against both



HM Government  
G-Cloud  
Supplier



IASME  
CYBER  
ASSURANCE



30+ five-star  
Google reviews



# Updates, access and malware protection

## 3 Security update management

- ☐ All software on in-scope devices is supported and licensed; Windows 10 without Extended Security Updates has been unsupported since 14 October 2025 **AUTOMATIC FAIL**
- ☐ Unsupported software removed, or the device moved out of scope into a segregated sub-set with no internet access
- ☐ Automatic updates enabled wherever possible
- ☐ High-risk and critical updates applied within 14 days of release: vendor-rated critical or high, no severity given, or CVSS v3 base score 7 or above; a bundled update containing any such fix counts **AUTOMATIC FAIL**
- ☐ The 14-day rule applied to firewall and router firmware, browsers and browser extensions, not only operating systems

## 4 User access control

- ☐ A documented process to create and approve user accounts
- ☐ Unique credentials for every user before access to applications, systems, services or devices
- ☐ Leaver and inactive accounts removed or disabled
- ☐ Admin rights and special privileges removed when no longer needed
- ☐ MFA enabled on every cloud service for all users and administrators wherever the service offers it, including through a paid tier; enforced at account level, not left as an optional setting **AUTOMATIC FAIL**
- ☐ Dedicated admin accounts for privileged tasks, with no email or web browsing from them
- ☐ Supplier, contractor and MSP accounts that manage your systems are in scope and meet the same rules
- ☐ Staff supported to choose unique passwords, with secure password storage provided
- ☐ A process to change passwords when a compromise is known or suspected

## 5 Malware protection

- ☐ A malware protection mechanism active on every in-scope device: anti-malware software (Windows and macOS) or application allow listing (any device)
- ☐ Anti-malware prevents malware and malicious code from running, and blocks connections to known malicious websites
- ☐ Anti-malware updated in line with vendor recommendations
- ☐ Where allow listing is used (common on phones and tablets): applications approved before deployment, a current list kept, and only code-signed applications run

**Not assessed:** backups (recommended by the NCSC, with restores tested), vulnerability assessment, penetration testing, logging and incident response all sit outside the scheme.



HM Government  
G-Cloud  
Supplier



IASME  
CYBER  
ASSURANCE



30+ five-star  
Google reviews



# Cyber Essentials Plus audit preparation

The requirements do not change at Plus. An IASME-licensed assessor tests them on sampled devices and every cloud service within 90 days of your basic certificate. Have the following ready.

- ☐ Written authorisation for testing, signed by someone with the authority to give it
- ☐ Plus scope matches the scope on your Cyber Essentials certificate exactly
- ☐ Where you certified a sub-set, segregation is real and demonstrable, not just documented
- ☐ Asset list (devices, operating systems, cloud services, public IP addresses) sent to your certification body so the sample can be set
- ☐ Sample set by the assessor per operating system (you do not choose it); users of sampled devices booked to be at them during testing, with sampled phones and tablets to hand
- ☐ On every sampled device: a working email client and browser, and a standard user account for the privilege check
- ☐ A standard user and an administrator account available for every cloud service, with MFA methods to hand for the observed sign-in
- ☐ Your certification body's test file domain and the assessor's sending address allow-listed in email and web filtering
- ☐ Every internet-facing IP address known, including IaaS; DNS names supplied where addresses are dynamic
- ☐ Access for the authenticated vulnerability scan set up and tested before the day on every sampled device, servers and IaaS included
- ☐ A technical contact (yours or your MSP's) with remote access to sampled devices, and someone who can sign in as administrator to each cloud service, available throughout
- ☐ High and critical vulnerabilities closed with the vendor fix or by removing the software; virtual patching is not accepted
- ☐ Verified self-assessment finalised; it is locked once testing starts and cannot be edited
- ☐ Audit and any retest completed within 90 days of the basic certificate; failed items fixed and retested within 30 days, and a second sample confirms the fix was applied across the whole scope

## Common pitfalls

- ✓ A personal phone with work email left out of scope, when it is in
- ✓ Firmware and browser extensions left out of the 14-day patching rule
- ✓ Starting too close to a tender deadline; replacing an unsupported device is a procurement timeline
- ✓ A cloud tool one team adopted without MFA, or a spare laptop or old server nobody remembered
- ✓ Answers that describe the policy rather than the configuration on the device



HM Government  
G-Cloud  
Supplier



IASME  
CYBER  
ASSURANCE



30+ five-star  
Google reviews



# Records, timeline and next steps

## Records to have ready

A few current records are all you need; at Plus the assessor compares them with what the scans and sampled devices show.

- |                                                                                           |                                                                                             |
|-------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| <input type="checkbox"/> Asset register: devices, operating systems, vendor support dates | <input type="checkbox"/> Cloud service inventory with MFA status against each entry         |
| <input type="checkbox"/> Admin account tracker, including MSP and contractor accounts     | <input type="checkbox"/> Scope statement defining the boundary and any sub-set              |
| <input type="checkbox"/> Patch and update record showing what was applied and when        | <input type="checkbox"/> Audit schedule agreed and users booked for the relevant test cases |
| <input type="checkbox"/> Device settings from MDM or group policy: lock and auto-run      | <input type="checkbox"/> Anti-malware console view, or the application allow list policy    |

## Prepare in two weeks

| Days            | What to do                                                                                                                                                                |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 to 3          | Agree scope and complete section 0. This is the step people skip, and it determines everything else.                                                                      |
| 4 to 7          | Clear the three automatic fails: vendor support, cloud MFA and the patch record.                                                                                          |
| 8 to 11         | Work through the remaining items per control and fix the gaps.                                                                                                            |
| 12 to 14        | Complete the question set with the checklist beside you, have someone else read the answers for contradictions, and have a director or board member sign the declaration. |
| If Plus follows | Book the Plus audit before you submit the basic assessment, so the 90-day window is not lost to scheduling.                                                               |

Reviewed by Harman Singh, IASME-licensed Cyber Essentials assessor, against the Danzell question set (v3.3), October 2026.

### Need a readiness check?

### Talk to an in-house IASME assessor.

We walk the five controls against your estate, automatic fails first, and hand you a ranked gap list before anything is submitted. Certification and Plus audits are delivered in-house too.

✉ [info@thecyphere.com](mailto:info@thecyphere.com)

☎ +44 (0) 333 050 9002

🌐 [thecyphere.com](https://thecyphere.com)



HM Government  
G-Cloud  
Supplier



30+ five-star  
Google reviews