A PRACTICAL CHECKLIST · CYBER ESSENTIALS READINESS

Cyber Essentials *Checklist.*

Readiness Self-Assessment

A six-section readiness self-assessment for IT managers, school business managers and service business leaders preparing for certification.

FOR SCHOOL AND BUSINESS IT TEAMS

Five controls.
Thirty-one checks.
One first-time pass.

SCOPE · FIREWALLS · SECURE CONFIGURATION · SECURITY UPDATES · USER ACCESS · MALWARE PROTECTION

Check the estate, then *answer the questions.*

This is a six-section readiness guide covering what must be true before you submit for Cyber Essentials. Built to be used as both a working plan and a record of what was checked, for the person who owns the outcome whether or not they hold an IT job title.

01 WHAT THIS IS

Six sections covering the ground an assessor will test: scope and assets, then each of the five technical controls (firewalls, secure configuration, security update management, user access control and malware protection). Thirty-one checks in total.

02 WHO IT IS FOR

IT managers and directors in multi-academy trusts, independent schools and further education colleges, school business managers who own compliance, and managing directors of service businesses asked for certification by a client or an insurer.

03 HOW TO MARK IT UP

For every check, mark whether the position is **In place**, **Partial**, or a **Gap**. Use the notes column to record the owner, the action required and the target completion date. Anything without a named owner should be escalated immediately.

04 HOW TO KEEP IT USEFUL

Run it before every submission and every renewal. A completed, dated copy is evidence for governors, trustees, auditors and insurers. Update it when devices, systems or the question set change.

CONTENTS

01 Scope and Asset Inventory p. 03

02 Firewalls p. 04

03 Secure Configuration p. 05

04 Security Update Management p. 06

05 User Access Control p. 07

06 Malware Protection p. 08

This checklist reflects Cyber Essentials requirements at the time of publication. Always confirm your answers against the current IASME question set before you submit.

SECTION 01 · OF SIX

Scope and Asset Inventory

Scope decides everything that follows. Complete this section before you open the question set.

6 CHECKS

Most failed submissions trace back to an incomplete asset list, not a weak control. Write down what is in scope before you assess anything.

#	CHECK	IN PLACE	PARTIAL	GAP	OWNER / NOTES
1	**Trigger and deadline recorded** *Insurance renewal, tender, college funding condition or trust review. Work back eight weeks from the date.*	☐	☐	☐	
2	**Scope defined and written down** *Whole organisation or a named subdivision. Whole-organisation scope is needed for the included cyber insurance (UK organisations under £20m turnover).*	☐	☐	☐	
3	**Device inventory complete** *Every laptop, desktop, tablet, mobile, server and network device, with operating system version and support end date.*	☐	☐	☐	
4	**Cloud services listed** *Every SaaS platform holding your data, including systems bought by departments without IT's knowledge.*	☐	☐	☐	
5	**Staff-owned and remote devices identified** *Personal phones and laptops used for work email or data are in scope. Record them.*	☐	☐	☐	
6	**Senior signatory named and briefed** *A board-level or equivalent representative must sign off. Brief them now, not on submission day.*	☐	☐	☐	

☐ In place: operates as documented

☐ Partial: exists but not fully operational

☐ Gap: absent or unverified

WHERE THIS TRIPS ORGANISATIONS UP

The asset list is usually built from memory rather than evidence. Pull it from your device management platform, your identity platform sign-in logs and your finance system's software subscriptions, then compare the three. The devices and services that appear in only one of those sources are the ones that fail submissions.

SECTION 02 · OF SIX

Firewalls

Covers every internet connection, including each site in a trust and every laptop used off-site.

5 CHECKS

Firewalls are usually in place. What fails is the configuration nobody has looked at since installation.

#	CHECK	IN PLACE	PARTIAL	GAP	OWNER / NOTES
1	**Boundary firewall on every internet connection** *Every site and every broadband circuit, including satellite buildings and temporary classrooms.*	☐	☐	☐	
2	**Default administrator password changed** *Replaced with a strong, unique password held in a secure password manager.*	☐	☐	☐	
3	**Admin interface not exposed to the internet** *Blocked from internet access, or protected by multi-factor authentication or an IP allow list where remote management is needed.*	☐	☐	☐	
4	**Inbound rules reviewed and documented** *Every open port has a recorded business reason. Remove any rule nobody can explain.*	☐	☐	☐	
5	**Software firewall enabled on mobile devices** *Laptops used at home or on public wi-fi need their own firewall switched on.*	☐	☐	☐	

☐ In place: operates as documented

☐ Partial: exists but not fully operational

☐ Gap: absent or unverified

A USEFUL QUESTION TO ASK

Who knows the firewall admin password, and when was it last changed? If the answer involves a supplier who left three years ago or a note taped inside the comms cabinet, you have found your first gap. Home routers used by remote staff are not in scope, which is exactly why the laptop's own firewall matters.

SECTION 03 · OF SIX

Secure Configuration

Printers, switches and firewalls count. Check every device with a login, not just laptops.

5 CHECKS

Secure configuration is about removing what you do not need. Default accounts, unused software and the open doors left by factory settings.

#	CHECK	IN PLACE	PARTIAL	GAP	OWNER / NOTES
1	**Default and unused accounts removed or disabled** *Including on printers, switches, firewalls and wireless access points.*	☐	☐	☐	
2	**Unnecessary software and services removed** *Uninstall anything with no business purpose, including trial software and pre-installed apps.*	☐	☐	☐	
3	**Auto-run disabled** *Removable media and downloaded files must not run automatically.*	☐	☐	☐	
4	**Device locking in place** *PIN, password or biometric to unlock, with protection against repeated guessing.*	☐	☐	☐	
5	**Password rules meet the current question set** *Minimum length combined with multi-factor authentication or automatic blocking of common passwords. Check this year's requirement, not last year's.*	☐	☐	☐	

☐ In place: operates as documented

☐ Partial: exists but not fully operational

☐ Gap: absent or unverified

WHERE THIS TRIPS ORGANISATIONS UP

Network kit is the blind spot. Laptops get reviewed because staff use them every day, while the printer on the second floor and the switch in the sports block are still running the credentials they shipped with. Walk the network, not just the device list.

SECTION 04 · OF SIX

Security Update Management

Fourteen days is the rule. Unsupported software is an automatic fail unless it is removed from scope.

5 CHECKS

This is the section where most schools and businesses discover the gap between what they believe is running and what actually is.

#	CHECK	IN PLACE	PARTIAL	GAP	OWNER / NOTES
1	**All software licensed and supported** *Operating systems, applications and firmware must be within vendor support.*	☐	☐	☐	
2	**Unsupported devices replaced, removed or segregated** *End-of-life iPads, Chromebooks past their auto-update expiry and unsupported Windows versions.*	☐	☐	☐	
3	**Critical and high-risk updates applied within fourteen days** *Updates rated critical or high by the vendor, applied within fourteen days of release on every in-scope device.*	☐	☐	☐	
4	**Automatic updates enabled wherever possible** *Manual patching is where the fourteen-day window slips.*	☐	☐	☐	
5	**Router and firewall firmware current** *Network device firmware is software. It is in scope and it needs patching.*	☐	☐	☐	

☐ In place: operates as documented

☐ Partial: exists but not fully operational

☐ Gap: absent or unverified

WHERE THIS TRIPS ORGANISATIONS UP

The tablet trolley is the classic fail. A set of iPads that has not been opened since the summer term can be several versions behind, and some will have dropped out of vendor support entirely. Charge them, update them and check support status before you answer the question set.

SECTION 05 · OF SIX

User Access Control

Multi-factor authentication on cloud services is not optional. This is the section where it gets checked.

5 CHECKS

Every account should belong to one person and carry only the access that person needs. Administrator access should be the exception, not the default.

#	CHECK	IN PLACE	PARTIAL	GAP	OWNER / NOTES
1	**Account creation and removal follows an approval process** *Joiners approved, leavers disabled promptly, including in third-party platforms.*	☐	☐	☐	
2	**Separate administrator accounts in use** *Admin accounts are used only for admin tasks, never for email or web browsing.*	☐	☐	☐	
3	**Admin rights removed from standard users** *Document who retains them and why. Review at least annually.*	☐	☐	☐	
4	**Multi-factor authentication on all cloud services** *Every cloud service that offers it, for all staff and every administrator account.*	☐	☐	☐	
5	**No shared or generic accounts** *Staffroom logins, a single admin account for the MIS and shared class accounts all need replacing.*	☐	☐	☐	

☐ In place: operates as documented

☐ Partial: exists but not fully operational

☐ Gap: absent or unverified

PRACTITIONER NOTE

Multi-factor authentication is usually switched on for IT staff first and never finished. Check the finance system, the MIS, HR platforms and any department-bought SaaS, not just Microsoft 365 or Google Workspace. One unprotected cloud account with admin rights is enough to fail the control.

SECTION 06 · OF SIX

Malware Protection

Covers every in-scope device type, including mobiles, tablets and staff-owned devices used for work.

5 CHECKS

Malware protection is rarely missing entirely. It is missing on the devices nobody thought to check.

#	CHECK	IN PLACE	PARTIAL	GAP	OWNER / NOTES
1	**Anti-malware active on all in-scope devices** *Or application allow-listing where anti-malware is not available for the platform.*	☐	☐	☐	
2	**Protection updates automatically** *Engine and signatures update without manual intervention.*	☐	☐	☐	
3	**Files scanned on access and malicious websites blocked** *Protection works at the point of use, not only on a scheduled scan.*	☐	☐	☐	
4	**Apps installed only from approved sources** *Tablets and phones limited to managed or official app stores.*	☐	☐	☐	
5	**Staff-owned devices meet the same standard** *Any personal device in scope needs equivalent protection. Confirm it, do not assume it.*	☐	☐	☐	

☐ In place: operates as documented

☐ Partial: exists but not fully operational

☐ Gap: absent or unverified

SUBMISSION READINESS GUIDE

Must be true before you open the question set: Scope written down, asset and cloud service list complete, senior signatory briefed, unsupported devices identified.

Must be true before you submit: Every gap in sections 02 to 06 closed, multi-factor authentication confirmed on all cloud services, patches current within fourteen days, answers reviewed and signed off.

Can follow certification: Cyber Essentials Plus decision within the three-month window, renewal date diarised, question set changes reviewed ahead of next year.

Operationalising the *checklist.*

The organisations that pass first time are not the ones with the biggest IT budgets. They are the ones that checked the estate before they answered the questions.

DMS SYSTEMS · IT FOR SCHOOLS AND BUSINESSES

i START WITH SCOPE

Write down what you are certifying before you assess anything. An incomplete asset list causes more failed submissions than any single weak control.

ii ASSIGN OWNERS

Every gap needs a named owner and a completion date, not just a flag. Use the notes column to record who is accountable. Anything without an owner gets escalated immediately.

iii EVIDENCE, NOT BELIEF

"We think we're probably fine" is not an answer an assessor accepts. Check the device, the setting and the account before you tick the box.

iv KEEP IT LIVE

Certification lasts twelve months and the question set changes. Keep a dated copy on file and rerun the checklist before every renewal.

ABOUT DMS

Here if a second opinion helps.

DMS supports IT managers, business managers and senior leaders in UK schools, multi-academy trusts and service businesses with network infrastructure, IT support and compliance, and holds Cyber Essentials certification itself. This checklist is a self-assessment tool you are welcome to use on its own. If a second opinion on any area would help, or you would rather someone ran the gap assessment with you, the details below are here to use.

CONTACT

dmsystem.co.uk

01322 420140

enquiries@dmsystem.co.uk

Design and Management Systems Limited · 2A-4 Avery Hill Road, New Eltham, London, SE9 2BD

Company Registered in England No [VERIFY] · VAT No: 863 6963 77 · Tel: 01322 420140

CYBER ESSENTIALS CERTIFIED · ISO 9001 · ISO 27001 · MICROSOFT SOLUTIONS PARTNER