TRANSCRYPT

The Ultimate Cyber Essentials Readiness Checklist

Audit your IT security against the UK Government's core standards.

About This Guide

Cyber Essentials is the UK Government-backed scheme that protects businesses against the most common cyber threats. Certification demonstrates your commitment to cyber security to your customers and stakeholders.

Transcrypt has created this self-assessment tool to help you benchmark your current IT setup against the five technical controls of Cyber Essentials.

How to Use This Document

1. **Audit:** Walk through the checklist on the following pages. Mark "Yes" only if you are 100% sure the requirement is met across **all** devices.
2. **Identify Gaps:** Any "No" answer represents a security gap.
3. **Remediate:** Use the **Action Plan** at the end of this document to assign fixes.
4. **Certify:** Once you have ticked every box, you are ready to apply for official certification with Transcrypt.

TRANSCRYPT

1. Firewalls

Objective: Ensure only safe and necessary network services can be accessed from the internet.

Requirement	Compliant?	Notes / Evidence
Boundary Firewalls: Is a firewall active on the network boundary (between your internal network and the internet)?	⬜ Yes ⬜ No	
Device Firewalls: Are software firewalls enabled on all devices (Windows Defender, macOS Firewall), particularly for remote workers?	⬜ Yes ⬜ No	
Default Passwords: Have all default administrative passwords on firewall/router interfaces been changed to strong, unique passwords?	⬜ Yes ⬜ No	
Inbound Connections: Are all inbound connections blocked by default unless explicitly documented and approved?	⬜ Yes ⬜ No	
Remote Access: Is RDP/SSH access secured behind a VPN or Multi-Factor Authentication (MFA)? (It must not be directly open to the internet).	⬜ Yes ⬜ No	

TRANSCRYPT

2. Secure Configuration

Objective: Computers and network devices are properly configured to reduce vulnerabilities.

Requirement	Compliant?	Notes / Evidence
Unnecessary Software: Has software not required for daily business work been removed from devices?	⬜ Yes ⬜ No	
Unnecessary Accounts: Have all unused, guest, or former employee accounts been removed or disabled?	⬜ Yes ⬜ No	
Auto-Run Disabled: Is 'Auto-run' or 'Auto-play' (for USBs/CDs) disabled on all systems?	⬜ Yes ⬜ No	
Strong Passwords: Are devices protected by strong passwords (min. 8 characters) or biometrics?	⬜ Yes ⬜ No	
Device Locking: Do devices auto-lock after a short period of inactivity (e.g., 5-15 minutes) requiring a password to unlock?	⬜ Yes ⬜ No	

TRANSCRYPT

3. User Access Control

Objective: Ensure user accounts are assigned to authorized individuals only.

Requirement	Compliant?	Notes / Evidence
Admin Separation: Do staff use standard user accounts for daily work (email/web), reserving Admin accounts *only* for administrative tasks?	⬜ Yes ⬜ No	
Account Management: Is there a formal process for creating and disabling user accounts (especially for leavers)?	⬜ Yes ⬜ No	
Multi-Factor Authentication (MFA): Is MFA enabled on ALL cloud services (Microsoft 365, Google Workspace, AWS, etc.)?	⬜ Yes ⬜ No	
Unique Credentials: Does every user have a unique username and password? (No shared accounts allowed).	⬜ Yes ⬜ No	

TRANSCRYPT

4. Malware Protection

Objective: Restrict the execution of known malware and untrusted software.

Requirement	Compliant?	Notes / Evidence
Anti-Malware Software: Is reputable anti-malware/antivirus software installed and active on all devices?	⬜ Yes ⬜ No	
Definition Updates: Is the software configured to update its signature database automatically (at least daily)?	⬜ Yes ⬜ No	
Real-Time Scanning: Is real-time scanning enabled to check files immediately upon access/download?	⬜ Yes ⬜ No	
Application Allow-listing: If AV is not used (e.g. on iOS), are only approved applications allowed to execute?	⬜ Yes ⬜ No	

TRANSCRYPT

5. Security Update Management (Patching)

Objective: Ensure that devices and software are not vulnerable to known security issues.

Requirement	Compliant?	Notes / Evidence
Supported Software: Are all operating systems and apps currently supported by the vendor? (You cannot use Windows 7, Server 2008, or old macOS versions).	⬜ Yes ⬜ No	
Automatic Updates: Are automatic updates enabled for both Operating Systems and installed applications?	⬜ Yes ⬜ No	
Critical Patching (14 Days): Are "Critical" or "High Risk" security patches applied within 14 days of release?	⬜ Yes ⬜ No	
Removal: Is unsupported software that cannot be updated removed from devices immediately?	⬜ Yes ⬜ No	

TRANSCRYPT

Remediation Action Plan

Use this table to log any "No" answers from the previous pages. These items must be fixed before you can achieve certification.

Control Area	Issue Description	Assigned To	Target Date	Fixed?
e.g., Access Control	*Administrator account used for email*	*John (IT)*	*Jan 20th*	⬜
				⬜
				⬜
				⬜
				⬜
				⬜

TRANSCRYPT

🛑 Need Help Fixing These Gaps?

Completing this checklist is the first step. If you found "No" answers and aren't sure how to fix them technically, Transcrypt can help.

We offer:

- **Gap Analysis:** Deep-dive verification of your systems.
- **Remediation Support:** We fix the issues for you.
- **Official Certification:** As a certification assistance organisation, we guide you through the official assessment.

Ready to Certify?

Contact our Cyber Essentials team today.

📧 Email: cyberessentials@transcrypt.com

🌐 Web: www.transcrypt.com

Disclaimer: This document is provided for guidance purposes only. Completion of this checklist does not guarantee a pass in the official Cyber Essentials assessment, but it is a strong indicator of readiness.