SmartSuite

Framework / Cybersecurity / Other

Cyber Essentials and Cyber Essentials Plus

Cyber Essentials is the NCSC-backed UK scheme of five technical controls; Cyber Essentials Plus adds independent technical testing. Requirements v3.3 applies from April 2026.



What it is

Cyber Essentials is the UK government-backed certification scheme, developed by the NCSC and delivered through its official delivery partner IASME, that checks whether an organization has put five technical controls in place: firewalls, secure configuration, security update management, user access control and malware protection. It comes in two levels. Cyber Essentials is a verified self-assessment; Cyber Essentials Plus covers the same controls and adds independent technical testing. The scheme has been used in government supply chains since 2014, and the current requirements document is version 3.3, published in April 2026.

The NCSC's Requirements for IT Infrastructure set out what the applicant must do. The applicant defines a scope boundary (the business unit, the network boundary and the physical location), agrees it with a Certification Body licensed by IASME, answers the question set, and has the answers signed off by a board member or equivalent before an assessor marks them.

At a glance

PUBLISHER NCSC (UK); IASME is the official delivery partner	TYPE Framework	VERSION Requirements for IT Infrastructure v3.3 (April 2026)
EFFECTIVE April 2026 (v3.3 requirements); scheme used in government supply chains since 2014	DOMAIN Cybersecurity	FAMILY Other
REGION United Kingdom	ADOPTION MODEL Certification	IMPLEMENTATION COMPLEXITY Low

Source: ncsc.gov.uk/cyberessentials/overview

Why it matters

- **A defined scope** Section D requires a scope boundary covering the business unit, the network boundary and the physical location, agreed with the Certification Body before assessment begins.
- **Five checkable controls** Section E states each control as requirements an assessor can mark, from firewall rules to the 14-day update window.
- **Independent verification** Answers are signed off by a board member or equivalent and marked by an assessor; Cyber Essentials Plus adds technical testing.
- **Cloud accountability** The applicant is always responsible for the controls on its cloud services, even where the provider implements them.

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports Cyber Essentials

Scope Boundary Register

Record the business unit, network boundary and physical location, any sub-sets, and the justification for a partial scope, with the Certification Body's agreement attached (section D).

Five-Control Requirement Library

Hold the firewall, secure configuration, security update, user access and malware requirements as controls with owners, status and linked evidence.

Cloud Service Responsibility Matrix

Track each cloud service as infrastructure, platform or software, who implements each control, and the contract clause that commits the provider, in Third Party Risk Management.

Update and Unsupported Software Tracking

Log critical and high-risk fixes against the 14-day window and list software that is no longer supported and must be removed or moved out of scope.

Account and MFA Review

Review user and administrator accounts, separate administrator accounts, removal of leavers and multi-factor authentication coverage for cloud services.

Assessment and Renewal Calendar

Plan the board sign-off, assessor questions, Plus testing remediation and the annual renewal that PPN 014 expects of suppliers.

Common framework mappings

CIS Controls v8.1 | ISO 27001:2022 | ISO 27002:2022 | NIST CSF 2.0 | NIST 800-53 Rev.5

Official resources

Cyber Essentials: Requirements for IT Infrastructure v3.3 (PDF)

The NCSC requirements document that applies from April 2026: scope rules and the five technical control themes.

ncsc.gov.uk/files/cyber-essentials-requirements-for-it-infrastructure-v3-3.pdf

Procurement Policy Note 014: Cyber Essentials scheme

The Cabinet Office note telling central government bodies when to require Cyber Essentials or Cyber Essentials Plus of suppliers.

gov.uk/government/publications/ppn-014-cyber-essentials-scheme

Cyber Essentials Scheme Overview

Outlines the structure and objectives of the Cyber Essentials certification program.

ncsc.gov.uk/cyberessentials/overview

Frequently asked questions

What is the difference between Cyber Essentials and Cyber Essentials Plus?

Both assess the same five technical controls. Cyber Essentials is a verified self-assessment: the answers are signed off by a board member or equivalent and marked by an assessor. Cyber Essentials Plus adds remote and on-site vulnerability testing to check that the controls defend against basic hacking and phishing attacks (PPN 014, Annex B). The NCSC lists Cyber Essentials from 320 pounds plus VAT, tiered by organization size, and prices Plus by the size and complexity of the network.

What changed in Requirements for IT Infrastructure v3.3?

The April 2026 document lists six changes: a definition of a cloud service, FIDO2 added to the definition of passwordless authentication, a firm statement that cloud services cannot be excluded from scope, the Software Security Code of Practice referenced in the software development section, the removal of untrusted connections from the scope criteria and a stronger emphasis on backing up data. Backups remain a recommendation rather than a technical requirement.

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

Which devices and cloud services are in scope?

Section D puts in scope every device and software that accepts incoming internet connections, makes outbound internet connections or controls the flow between them. End-user devices must be included, as must cloud services holding organizational data or services, and user-owned devices that reach organizational data. Devices used only for native voice, text or authenticator apps are out. A partial scope needs a justification the assessor will test.

How fast must updates be applied, and what authentication is required?

Section E.3 requires software to be licensed and supported, with critical or high-risk fixes (a CVSS v3 base score of 7 or above, or the vendor's own critical or high-risk rating) applied within 14 days of release. Section E.4 requires multi-factor authentication wherever it is available, and always for cloud services. Passwords need multi-factor authentication, or at least 12 characters, or at least 8 characters with a deny list of common passwords.

Do UK government suppliers have to hold Cyber Essentials?

Not in every case. PPN 014, updated February 2025, tells central government departments, executive agencies, non-departmental public bodies and NHS bodies to require Cyber Essentials or Cyber Essentials Plus, or equivalent controls, on contracts that involve citizens' personal information, government staff information or OFFICIAL-level data. It warns against a blanket approach, says certification must be renewed annually where required, and notes that Cyber Essentials does not assure the specific product or service supplied.

License included / downloadable: Yes The Requirements for IT Infrastructure and the question set are published free by the NCSC and are UK Crown copyright. Certification itself is paid and priced by organization size; the platform links to the official documents.

Full framework page and mappings: smartsuite.com/frameworks/uk-cyber-essentials-plus