

Cyber Essentials Cyber Essentials Plus

Cyber Essentials is a UK government-backed certification specifying basic controls to protect organizations against common cyber threats.



What it is

Cyber Essentials is a UK government-backed cybersecurity certification scheme that helps organizations protect against common cyber threats and demonstrate a minimum level of cyber resilience. The framework provides a set of foundational security controls designed to reduce the risk of prevalent attacks and safeguard sensitive information.

Published by the UK National Cyber Security Centre (NCSC), Cyber Essentials is widely adopted by businesses, non-profits, and public sector organizations seeking to improve their basic cybersecurity posture. The scheme covers five key technical control areas: firewall configuration, secure settings, access control, malware protection, and patch management, offering a baseline for organizational security practices.

At a glance

PUBLISHER National Cyber Security Centre (NCSC)	TYPE Framework	VERSION Current Cyber Essentials Certification Scheme
EFFECTIVE 2014	DOMAIN Cybersecurity	FAMILY Other
REGION United Kingdom	ADOPTION MODEL Certification	IMPLEMENTATION COMPLEXITY Moderate

Source: <https://www.cyberessentials.ncsc.gov.uk>

Why it matters

- Strengthen security oversight** Support consistent implementation and management of core technical controls across the organization's digital infrastructure.
- Enhance regulatory alignment** Demonstrate adherence to government-endorsed security standards and streamline compliance with public sector and contractual requirements.
- Promote operational resilience** Reduce the risk of common cyber incidents by proactively addressing vulnerabilities in systems, networks, and devices.
- Increase audit readiness** Facilitate efficient evidence gathering and validation for certification, supporting internal and third-party assurance activities.

How SmartSuite supports Cyber Essentials

Baseline Control Checklist Track the five control areas with owners, scope, and implementation status.	Asset Inventory and Coverage Define endpoints, servers, and networks in scope for certification readiness.	Evidence Collection for Certification Centralize configuration proof, patching evidence, and access control artifacts.
Gap and Exception Management Track gaps, corrective actions, and exceptions with approval and closure evidence.	Patching and Configuration Review Schedule Schedule patching, malware protection checks, and configuration reviews.	Certification Readiness Reporting Report control status and open items for assessment preparation.

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 Technical Requirements Provides detailed specifications for implementing Cyber Essentials controls and achieving certification. nsc.gov.uk/files/cyber-essentials-requirements-for-it-infrastructure-v3-2.pdf	Cyber Essentials Scheme Overview Outlines the structure and objectives of the Cyber Essentials certification program. nsc.gov.uk/cyberessentials/overview
Cyber Essentials Implementation Guide Describes practical guidance on implementing Cyber Essentials controls within an organization. nsc.gov.uk/cyberessentials/overview	

Frequently asked questions

- What is UK Cyber Essentials used for?**

UK Cyber Essentials is designed to help organizations protect themselves against common cybersecurity threats by implementing essential technical controls. It provides a standardized framework to demonstrate a basic level of cyber resilience and is often used to meet supply chain and regulatory requirements.
- Is UK Cyber Essentials certification mandatory?**

Cyber Essentials certification is not legally mandatory for all organizations, but it is a requirement for many UK government contracts and public sector tenders. Many private sector organizations also adopt it to demonstrate due diligence in cybersecurity and meet third-party risk management expectations.
- What organizations are in scope for UK Cyber Essentials?**

UK Cyber Essentials is applicable to any organization, regardless of size or sector, that uses internet-connected IT infrastructure and wants to demonstrate foundational cybersecurity. Organizations handling sensitive data, or providing goods and services to UK government entities, are particularly encouraged or required to comply.
- What are the five core technical controls of UK Cyber Essentials?**

The scheme requires implementing five key technical controls: firewall and internet gateway configuration, secure configuration of devices, user access control (such as strong password policies), malware protection, and patch management. These controls are intended to mitigate the most common cyber threats.

How does an organization achieve UK Cyber Essentials certification?

Organizations must implement the required controls, complete a self-assessment questionnaire, and submit it to an accredited certification body for review. For a higher level of assurance, Cyber Essentials Plus includes independent technical verification in addition to self-assessment.

How does UK Cyber Essentials relate to other cybersecurity frameworks?

UK Cyber Essentials provides a baseline of basic controls and is often used in conjunction with more comprehensive frameworks like ISO 27001 or the NIST Cybersecurity Framework. While Cyber Essentials focuses on essential hygiene measures, other frameworks may address broader information security governance and risk management.

What are the ongoing compliance requirements for UK Cyber Essentials?

Certification is valid for 12 months, after which organizations must renew by reassessing their environment and verifying continued compliance with the controls. Organizations are expected to continuously monitor, update, and improve their security controls to address evolving threats.

How would SmartSuite support UK Cyber Essentials?

SmartSuite streamlines Cyber Essentials compliance management by mapping framework requirements to a centralized control library, tracking implementation status, and organizing policy documentation. It enables evidence collection for each control, monitors risks, supports audit readiness, and provides reporting dashboards to maintain certification and demonstrate ongoing compliance.

License included / downloadable: Yes Cyber Essentials documentation and certification guidance are publicly available through the UK National Cyber Security Centre and official program providers.

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