

The SME Cyber Compliance Readiness Guide

CAF • ISO 27001 • Cyber Essentials Plus • Cyber Insurance

A practical guide to understanding what you're being asked to demonstrate, where organisations commonly get stuck, and how to move from a standing start towards audit-ready evidence.

CERTIFICATION IS MORE THAN POLICIES

Policies are one layer. The real question is whether controls operate and can be demonstrated.



The strongest organisations keep these layers connected and current.

A policy saying “we test backups” is not the same as evidence that a restore test happened.

2026 Edition • CyberSec Compliance Ltd • cyberseccompliance.co.uk

1. Why this guide exists

Most organisations don't set out to "get certified" for its own sake. Something external usually asks for it first: a public-sector tender demanding CAF alignment, an enterprise customer's vendor security assessment referencing ISO 27001, a cyber-insurance renewal with tighter underwriting questions, or a customer simply asking whether you are Cyber Essentials certified.

The important question is not simply "Do we have the policy?" It is "Can we demonstrate that the requirement is understood, implemented and operating?"

WHICH ROUTE IS RIGHT FOR YOUR BUSINESS?

A practical starting point — the requirement usually comes from an external business need.

CUSTOMER / TENDER REQUIREMENT

ISO 27001

A customer or contract asks for a formal information-security management system.

PUBLIC-SECTOR / SECTOR REQUIREMENT

CAF

A resilience framework is required or expected in your sector or regulatory environment.

BASELINE CYBER ASSURANCE

CYBER ESSENTIALS

You need the UK Government-backed baseline for core technical controls.

INDEPENDENT TECHNICAL ASSURANCE

CE+

You need the technical verification that sits on top of Cyber Essentials.

INSURANCE REQUIREMENT

CYBER INSURANCE READINESS

You need confidence in your controls, answers and supporting evidence.

2. CAF — the resilience view

The NCSC Cyber Assessment Framework (CAF) is a resilience framework rather than a certification you buy from an accredited body. It is usually applied through self-assessment or assessed by a sector regulator. It is structured around four Objectives, 14 Principles and contributing outcomes.

CAF • THE RESILIENCE VIEW

The NCSC Cyber Assessment Framework is structured around four Objectives, 14 Principles and contributing outcomes.

01

MANAGING SECURITY RISK

Understand what matters, who is responsible and how risk is managed.

02

PROTECTING AGAINST CYBER ATTACK

Put appropriate protective measures around systems, people and information.

03

DETECTING CYBER SECURITY EVENTS

Have the capability to identify relevant events and understand what is happening.

04

MINIMISING THE IMPACT OF INCIDENTS

Contain, respond, recover and learn from incidents.

Where organisations get stuck

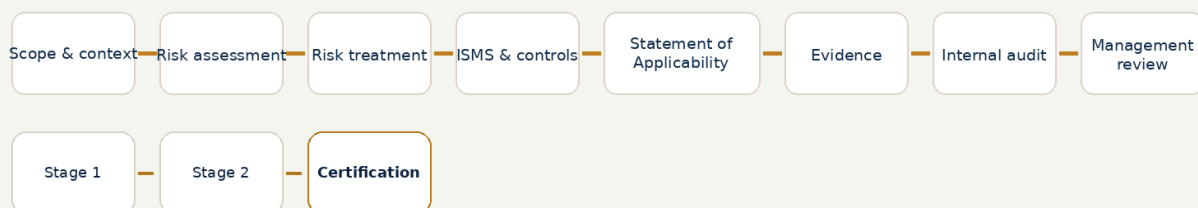
- Treating CAF as a one-off document exercise rather than an ongoing resilience posture.
- Confusing the existence of a technical control with evidence that it is actually operating.
- Underestimating the management and governance elements that sit alongside technical controls.

3. ISO 27001 — the management system journey

ISO 27001 certification is issued by an independent accredited certification body following formal external audit. The organisation controls its Information Security Management System (ISMS), including its policy set, Statement of Applicability and management-system requirements covering context, leadership, planning, support, operation, performance evaluation and improvement.

ISO 27001 • THE MANAGEMENT SYSTEM JOURNEY

Certification is performed by an independent accredited certification body; CyberSec supports the preparation and evidence journey.



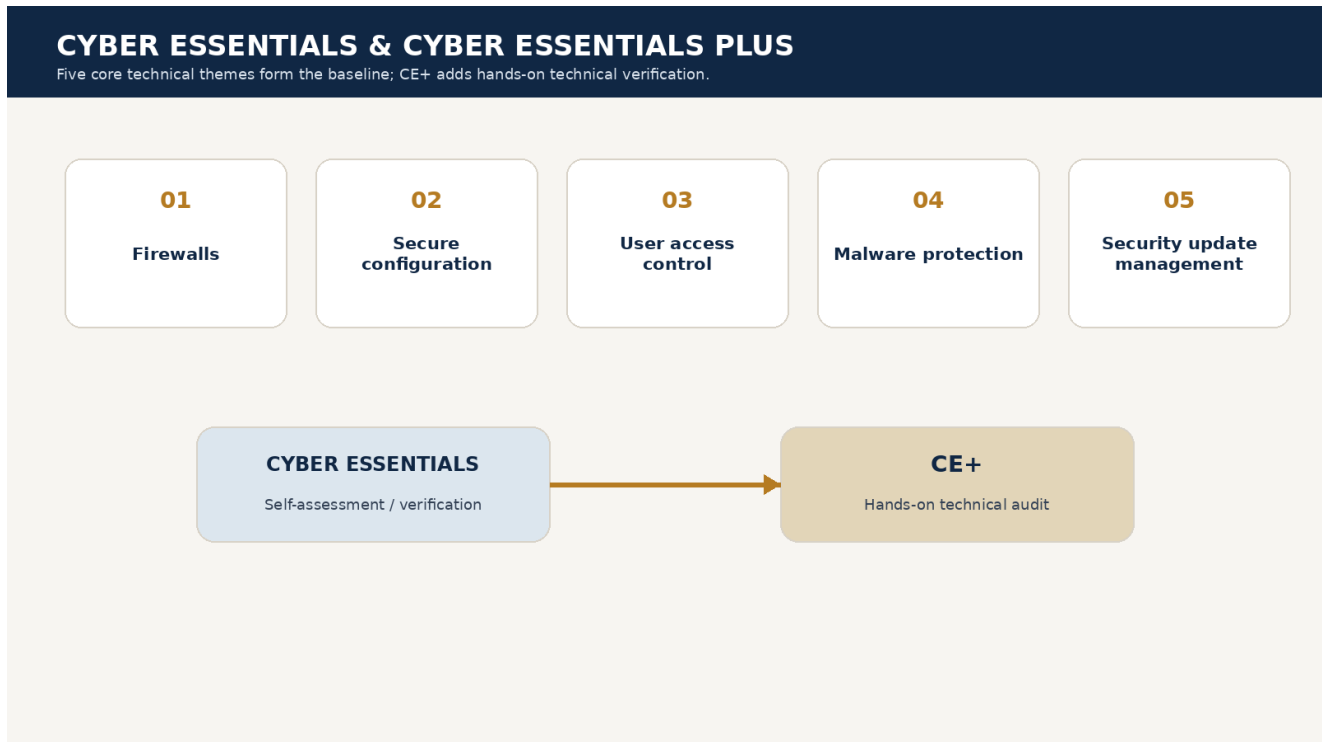
ISO 27001 is an ISMS: management requirements + risk + controls + evidence + continual improvement.

Where organisations get stuck

- Generic policies that do not reflect how the business actually operates.
- A Statement of Applicability that has not genuinely been reviewed control-by-control.
- No meaningful internal-audit schedule or management-review records.

4. Cyber Essentials & Cyber Essentials Plus

Cyber Essentials is the UK Government-backed baseline, covering five technical control themes: firewalls, secure configuration, user access control, malware protection and security update management. Cyber Essentials Plus adds hands-on technical verification of those controls.



Where organisations get stuck

- Answering questions about how things should work rather than how they actually work.
- Underestimating the scope of BYOD where personal devices access company data.
- Failing to address unpatched or internet-facing systems before CE+ technical testing.

5. Cyber insurance readiness

Insurance underwriting questions increasingly focus on practical controls and evidence. The areas highlighted in this guide include MFA enforcement, backup-testing frequency, incident-response planning and supplier risk management.

CYBER INSURANCE READINESS

Good answers are backed by current evidence — not memory or optimistic assumptions.



DON'T WAIT UNTIL RENEWAL

Maintain evidence continuously so underwriting questions can be answered confidently.

Where organisations get stuck

- Completing insurer questionnaires from memory rather than from current evidence.
- Having a plan on paper but no practical incident-response preparation.
- Discovering gaps only when renewal is due and time is limited.

6. The evidence gap

Across all four areas, a recurring problem is the gap between documentation and reality. A policy may describe an intended control, but an assessor, customer or insurer may need evidence that the control is actually operating.

THE EVIDENCE GAP

The difference between saying a control exists and demonstrating that it operates.

"We have backups."



Backup configuration + records

"MFA is enabled."



Configuration / coverage evidence

"We test restores."



Completed restore-test records

"We train staff."



Training / awareness records

"We have an incident plan."



Plan + exercise / review evidence

The practical rule

Treat your policy set as a living reflection of real practice — not a compliance exercise completed once and filed away.

7. The CyberSec approach

CyberSec is designed around the connection between assessment, requirements, remediation and evidence. One guided questionnaire can provide a common starting point for multiple compliance and assurance needs.

THE CYBERSEC APPROACH

One guided assessment, connected to the work that follows.



The objective is continuity: keep the compliance picture current as the organisation, technology and requirements change.

8. A practical starting checklist

Before you begin a certification or insurance-readiness programme, make sure you can identify:

- What systems, devices, users and information are in scope.
- Who owns information-security decisions and risk.
- What technical controls are actually deployed.
- Which controls require improvement or remediation.
- What evidence exists to demonstrate operation.
- Which policies and procedures need updating.
- Which actions have owners and target dates.
- How incidents, backups, access and supplier risks are managed.
- How reviews, testing and improvement will be maintained over time.

CERTIFICATION IS MORE THAN POLICIES

Policies are one layer. The real question is whether controls operate and can be demonstrated.



The strongest organisations keep these layers connected and current.

A policy saying “we test backups” is not the same as evidence that a restore test happened.

READY TO SEE WHERE YOU STAND?

Find the gaps before an assessor, customer or insurer finds them.

TAKE THE FREE

CYBERSEC READINESS ASSESSMENT

Get a practical view of your current readiness
and the actions that matter most.

cyberseccompliance.co.uk

About CyberSec Compliance

CyberSec Compliance provides a guided platform for SMEs working towards stronger cyber governance, certification readiness and insurance readiness. The platform is designed to connect assessment answers with requirements, policies, risks, actions and evidence rather than treating documentation as a standalone exercise.

Important: CyberSec does not itself issue ISO 27001 certification or replace an independent certification body, regulator or assessor. The purpose of this guide is to help organisations understand the preparation and evidence journey.

CyberSec Compliance Ltd • cyberseccompliance.co.uk • info@cyberseccompliance.co.uk