SmartSuite

Framework / Cybersecurity / Other

NCSC Cyber Assessment Framework (CAF) version 4.0

The NCSC Cyber Assessment Framework (CAF v4.0) has 4 objectives, 14 principles and 41 contributing outcomes for assessing cyber resilience of essential functions, used by UK regulators.



What it is

The Cyber Assessment Framework (CAF) is the outcome-based framework, published by the NCSC as the UK's national technical authority for cyber security, for judging how well an organization manages cyber risk to its essential functions. This page follows version 4.0, released on August 4, 2025; the version 3.1 named in the page title (April 11, 2022) was superseded by version 3.2 (April 15, 2024) and then by version 4.0. The CAF is designed for organizations that run essential services in energy, healthcare, transport, digital infrastructure and government, and for the regulators that oversee them.

The CAF has four objectives, 14 principles and 41 contributing outcomes. Each outcome is judged against Indicators of Good Practice (IGPs) and graded achieved, partially achieved or not achieved, and the result is compared with a CAF profile, which sets the target level for a sector. Regulators under the Network and Information Systems (NIS) Regulations use it, and so does GovAssure, the assurance scheme for the critical systems of UK government organizations.

At a glance

PUBLISHER National Cyber Security Centre (NCSC)	TYPE Framework	VERSION Version 4.0 (supersedes v3.2, April 15, 2024, and v3.1, April 11, 2022)
EFFECTIVE August 4, 2025 (v4.0 release)	DOMAIN Cybersecurity	FAMILY Other
REGION United Kingdom	ADOPTION MODEL Voluntary	IMPLEMENTATION COMPLEXITY High

Source: ncsc.gov.uk/collection/cyber-assessment-framework

Why it matters

- **Outcomes, not a checklist** The 4 objectives and 14 principles specify what must be achieved, and the IGPs inform expert judgment rather than replacing it.
- **A target level, not a perfect score** A CAF profile selects the outcomes that must be achieved or partially achieved at a given attacker capability, so not every outcome needs a green result.
- **Self-assessment or independent review** Assessments can be done by the organization or by an external body such as a regulator or an NCSC assured provider.
- **Threat-informed risk decisions** Version 4.0 principle A2.b asks the organization to understand threat actor capabilities, methods and techniques and use them in risk decisions.

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports UK CAF v3.1

Outcome and IGP Library

Load the 4 objectives, 14 principles and 41 contributing outcomes with their achieved, partially achieved and not achieved indicators, and record the judgment for each.

Profile and Target Tracking

Record the CAF profile or regulator expectation that applies and compare each outcome's current judgment with its target.

Threat Understanding Register

Capture the threat analysis behind A2.b, linking threat actors, methods and the systems supporting essential functions to risk decisions in Cyber & IT Risk.

Software and Supplier Assessments

Assess suppliers and software provenance for A4.a and A4.b in Third Party Risk Management, with secure development evidence.

Detection and Threat Hunting Evidence

Log monitoring coverage, alert triage and threat hunts for C1 and C2, with findings and follow-up actions.

Response, Recovery and Lessons Learned

Link D1 response plans, exercises and D2 post-incident reviews to incident records and improvement actions in Operational Resilience & Business Continuity.

Common framework mappings

CIS Controls v8.1 | Cyber Essentials | ISO 27001:2022 | ISO 27002:2022 | ISO 27701 | MITRE ATT&CK | NIST CSF 2.0 | NIST 800-53 Rev.5

Official resources

NCSC Cyber Assessment Framework (CAF) v4.0 collection

The NCSC's CAF collection: the v4.0 objectives, principles, contributing outcomes and indicators of good practice, the changelog and the PDF.

ncsc.gov.uk/collection/cyber-assessment-framework

Frequently asked questions

Which version of the CAF is current and what changed?

Version 4.0, released on August 4, 2025, replaced version 3.2 (April 15, 2024), which had replaced version 3.1 (April 11, 2022). The NCSC lists four major changes: a new section on attacker methods and motivations (A2.b), a new section on secure software development and support (A4.b), updated security monitoring and threat hunting (C2 is now Threat Hunting), and improved coverage of AI-related cyber risks.

How is the CAF structured?

The CAF has four objectives (A Managing security risk, B Protecting against cyber attack, C Detecting cyber security events, D Minimising the impact of cyber security incidents) and 14 principles. The principles break into 41 contributing outcomes, and each outcome has a table of Indicators of Good Practice.

How is a contributing outcome judged?

An assessor uses the IGP table to decide achieved, partially achieved or not achieved. All the achieved indicators would normally be present for achieved, and any one not achieved indicator would normally justify not achieved. The NCSC says IGPs inform expert judgment and are not an inflexible checklist.

What are CAF profiles?

A CAF profile is a target level of cyber security and resilience against attackers of a particular capability. The Basic Profile applies to all sectors against basic attack capability, and an Enhanced Profile is sector-specific and builds on the Basic Profile; regulators set these targets for their sectors.

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

Who uses the CAF?

The NCSC designed it for organizations operating essential services in sectors such as energy, healthcare, transport, digital infrastructure and government, including those regulated under the NIS Regulations. The NCSC says nearly all UK cyber regulators use it and that GovAssure applies it to the critical systems of government organizations.

License included / downloadable: Yes The CAF is a free download from the NCSC. Its text is Crown copyright and is released for re-use under version 3.0 of the UK's Open Government terms, as the document's closing notice states; photographs and infographics are not available for re-use.

Full framework page and mappings: smartsuite.com/frameworks/uk-cyber-assessment-framework-caf