NCSC Cyber Assessment Framework v4.0 implementation guide

The NCSC Cyber Assessment Framework (CAF) stands as the UK's primary cybersecurity assessment standard for critical national infrastructure, with version 4.0 released on August 6, 2025, representing the most significant update since its 2018 inception. CM Alliance +5 Unlike the control-based approaches of ISO 27001 or NIST CSF, CAF employs an outcome-focused methodology specifically designed for Operators of Essential Services (OES) under NIS Regulations, CM Alliance Clearcutcyber covering both IT and operational technology environments through 4 objectives, 14 principles, and 41 contributing outcomes evaluated against 551 Indicators of Good Practice. The Cyphere +2

The framework fundamentally differs from traditional compliance approaches by prioritizing security outcomes over prescribed controls, allowing organizations to determine their own implementation methods while meeting regulatory requirements. CM Alliance +2 This flexibility, combined with explicit coverage of operational technology and sector-specific adaptations, makes CAF particularly valuable for critical infrastructure operators in energy, healthcare, transport, water, digital infrastructure, and government sectors Sapphire.net Open Access Government who must demonstrate cyber resilience to sector regulators.

Framework architecture and component hierarchy

The CAF structure follows a clear hierarchical model from high-level objectives down to detailed indicators. **Four core objectives** form the foundation: Objective A focuses on Managing Security Risk through appropriate organizational structures and systematic risk management; Objective B addresses Protecting Against Cyber Attack with proportionate security measures; Objective C covers Detecting Cyber Security Events to maintain effective defenses; and Objective D ensures capabilities for Minimising the Impact of Cyber Security Incidents including service restoration. UK Government Security

These objectives cascade into **14 principles** that define specific security domains. Under Objective A, organizations address A1 Governance, A2 Risk management, A3 Asset management, and A4 Supply chain. Objective B encompasses the majority with B1 Service protection policies and processes, B2 Identity and access control, B3 Data security, B4 System security, B5 Resilient networks and systems, and B6 Staff awareness and training. Objective C contains C1 Security monitoring and C2 Proactive security event discovery, while Objective D includes D1 Response and recovery planning and D2 Lessons learned. UK Government Security

Each principle breaks down into **contributing outcomes** using a hierarchical identifier system (A1.a, A1.b, B2.a, etc.), totaling 41 specific requirements in version 4.0. The assessment of these outcomes relies on **Indicators of Good Practice (IGPs)** organized in three-column tables showing characteristics for "Not Achieved," "Partially Achieved," and "Achieved" states. Wallarm +2 With 551 total IGPs including 108 additions in v4.0, Bridewell bridewell these provide detailed guidance while maintaining flexibility for sector-specific interpretation and alternative control implementations.

The framework employs **CAF Profiles** to set target achievement levels appropriate to different threat environments. The Baseline Profile establishes minimum standards for common threats, while the Enhanced Profile sets higher requirements for organizations facing advanced persistent threats. [UK Government Security] Competent Authorities can create sector-specific profiles that mix achievement levels across contributing outcomes based on risk assessments and regulatory requirements.

Assessment methodology and scoring system

CAF assessment operates through an outcome-focused methodology that explicitly avoids tick-box compliance exercises, instead requiring expert judgment informed by IGPs. [The Cyphere] [Industrial Cyber] Organizations receive **41 individual assessments**, one per contributing outcome, using a three-tier scale where "Not Achieved" indicates the presence of any negative indicator, "Partially Achieved" demonstrates partial controls delivering specific benefits, and "Achieved" requires all positive indicators to be typically present with no negative indicators true.

The IGP evaluation process treats indicators as **guidance tools rather than inflexible requirements**, allowing organizations to demonstrate alternative controls that achieve the same security outcomes. Assessment involves reviewing evidence against IGP tables, applying professional cybersecurity expertise to determine achievement levels, documenting rationale for ratings including any compensating controls, and considering sector-specific circumstances and threat contexts. If any indicator in the "Not Achieved" column is true, that outcome cannot be rated higher regardless of other positive indicators present. [Bridewell] [2T Security]

Organizations can pursue either **self-assessment or independent assessment** approaches. Self-assessment leverages internal expertise and organizational knowledge while promoting ownership of cybersecurity improvements, though it requires appropriate expertise and objective evaluation with comprehensive documentation. Independent assessment by NCSC-assured providers or regulatory bodies provides external validation and may be required by sector regulators, offering professional verification of organizational claims against evidence. [Industrial Cyber]

The **WebCAF platform** serves as the primary assessment tool, particularly for government sector assessments under GovAssure. [2T Security] This bespoke platform provides role-based access control for organization, system, and assessor levels, enables collaborative assessment with multiple contributors, supports evidence repository management with cross-referenced documentation, and generates assessment summaries and improvement tracking reports. [UK Government Security] Documentation requirements include cyber strategies and policies, governance structures, asset inventories, architecture diagrams, assessment records, and evidence of controls implementation.

Version 4.0 updates and enhancements

The August 2025 release of CAF v4.0 introduces the most substantial changes since the framework's creation, responding to evolving cyber threats and emerging technologies. [Industrial Cyber +2] **New contributing outcome A2.b "Understanding Threat"** requires organizations to maintain documented threat analysis methodologies including attack scenario modeling using attack trees, threat intelligence consumption aligned to business context, and understanding of relevant threat actors and their techniques. [Sapphire.net +2]

Enhanced software security requirements appear in new outcome A4.b covering secure software development lifecycle, demanding code provenance tracking and software bill of materials maintenance, static and dynamic code analysis implementation, supplier evidence of secure development frameworks (specifically referencing NIST SSDF and Microsoft SDL), and continuous monitoring of third-party component vulnerabilities. [Bridewell] [bridewell] These additions reflect lessons from supply chain attacks like SolarWinds and increasing software complexity in critical infrastructure.

The framework now explicitly addresses **artificial intelligence risks** through references to "automated decision-making technologies" embedded throughout risk management processes. [Bridewell] [bridewell] Organizations must consider AI-specific threats in their risk assessments, implement controls for AI system security and reliability, and maintain governance oversight of automated decision-making systems affecting essential services. [Sapphire.net]

Advanced threat hunting capabilities receive significant emphasis through the complete rewrite of C2.b (renamed from "Proactive Active Discovery" to "Threat Hunting") and new outcome C1.f focusing on understanding user and system behavior. [Bridewell] [bridewell] These changes promote adoption of an "assumed breach" mentality, structured threat hunting methodologies, risk and intelligence-led hunting approaches, and behavioral analytics for anomaly detection.

Implementation guidance and best practices

Successful CAF implementation begins with thorough preparation involving stakeholder identification across system owners, cybersecurity teams, and governance leads. Organizations should **invest in training** to ensure assessors understand CAF structure, interpretation flexibility, and the importance of expert judgment over checkbox compliance. Evidence collection should focus on gathering existing documentation rather than creating new materials specifically for assessment, recognizing that CAF evaluates actual security practices rather than documentation quality.

The assessment execution follows a **phased approach** starting with Objective A (governance and risk management) to establish organizational context before proceeding through technical controls in Objectives B and C, concluding with incident response capabilities in Objective D. Regular checkpoint meetings ensure quality and consistency across assessors, while the collaborative features of assessment tools enable appropriate division of responsibilities among subject matter experts.

Organizations should **leverage existing framework implementations** where possible, as NCSC provides official mapping between CAF and other standards. Those with ISO 27001 certification or NIST CSF implementations can use these as starting points, documenting how existing controls meet CAF outcomes. The key lies in translating control-based implementations into outcome achievements, ensuring coverage of CAF-specific requirements like OT security and essential service continuity.

For **continuous improvement**, organizations should treat CAF assessment as an ongoing process rather than a one-time activity. Regular reassessment cycles, typically annual for OES, identify emerging gaps as threats evolve and systems change. Improvement roadmaps should prioritize remediation based on risk to essential services, focusing first on "Not Achieved" outcomes that pose the greatest threat to service continuity.

Comparison with ISO 27001 and NIST frameworks

CAF's outcome-focused approach contrasts sharply with ISO 27001's prescriptive control requirements, offering **greater implementation flexibility** while maintaining rigorous security standards. Where ISO 27001 mandates specific controls from its 93-control Annex A, CAF defines desired security outcomes and allows organizations to determine appropriate implementation methods. [OneTrust] This philosophical difference extends to assessment, with CAF using expert judgment against outcomes rather than audit checklists against controls.

The framework shares NIST CSF's risk-based approach and five-function model (Identify, Protect, Detect, Respond, Recover) but differs in application context and regulatory backing. [TechUK] [Clearcutcyber] **CAF explicitly supports UK regulatory compliance** for essential services under NIS Regulations, while NIST CSF provides voluntary guidance without regulatory mandate. [OneTrust] [2T Security] CAF's 4-objective structure maps conceptually to NIST's functions but includes specific requirements for critical infrastructure protection and operational technology security often absent from NIST implementations.

Unlike both ISO 27001 and NIST CSF, CAF **comprehensively addresses IT/OT convergence** from inception. The framework recognizes that essential services increasingly depend on cyber-physical systems where traditional IT security approaches prove insufficient. CAF requirements explicitly cover industrial control systems, SCADA networks, and operational technology environments, demanding integrated security approaches that span both domains while respecting operational constraints and safety requirements.

Organizations often adopt a **complementary multi-framework strategy**, using CAF for regulatory compliance and maturity assessment while maintaining ISO 27001 certification for market credibility and implementing NIST CSF's structured approach for program development. [Hicomply] This approach maximizes value from existing investments while meeting specific UK regulatory requirements through CAF assessment.

Essential services and OES focus areas

CAF specifically targets organizations providing essential services across six critical sectors defined by NIS Regulations. [Itgovernance +2] **Energy sector** organizations including oil, gas, and electricity operators must address both cyber and physical security with special emphasis on operational technology protecting generation and distribution systems. [Hicomply] The framework's DGE (Downstream Gas and Energy) overlay adds "Objective E" covering physical security requirements unique to energy infrastructure. [2T Security]

Healthcare providers implement CAF with additional IGPs addressing secure data transmission and patient privacy protection, recognizing the life-critical nature of medical services and sensitive personal data involved. Transport operators in aviation, rail, shipping, and cargo apply sector-specific CAF versions that consider safety-critical systems where cyber incidents could cause physical harm. 2T Security Water utilities focus on protecting treatment and distribution systems essential for public health, while digital infrastructure providers securing DNS services, Internet Exchange Points, and TLD registries emphasize availability and integrity given their foundational role in digital communications.

Government organizations utilize CAF through the GovAssure scheme with WebCAF portal access for secure assessment submission. UK Government Security 2T Security Local authorities implementing CAF must consider their dual role as service providers and data controllers, addressing both operational resilience and citizen data protection. The framework's flexibility allows each sector to emphasize relevant aspects while maintaining consistent assessment methodology across all essential services.

Competent Authorities designated for each sector oversee CAF implementation with varying approaches to profile setting and assessment requirements. Most have aligned to CAF as their primary assessment framework, 2T Security though some like Ofgem have enhanced requirements reflecting sector-specific threats. 2T Security The Civil Aviation Authority developed "CAF for Aviation" with additional safety-critical system considerations, 2T Security demonstrating the framework's adaptability to sector needs while maintaining core assessment consistency. bridewell 2T Security

Operational technology and IT/OT convergence

CAF's comprehensive OT coverage distinguishes it from traditional IT security frameworks, explicitly requiring organizations to **secure industrial control systems** including SCADA networks, distributed control systems, programmable logic controllers, and human-machine interfaces. The framework recognizes that these systems often operate with different constraints than enterprise IT, including continuous availability requirements, extended lifecycle spanning decades, limited patching windows, and safety considerations overriding security in some contexts.

IT/OT convergence challenges receive specific attention through requirements for **unified security governance** spanning both domains. Organizations must establish clear accountability for OT security, often requiring new reporting structures bridging traditional IT security and operational engineering teams. Risk assessment processes must consider cascading effects where IT compromises could impact OT systems and physical processes, while security monitoring must provide visibility across interconnected IT/OT environments without disrupting critical operations.

The framework promotes **defense-in-depth strategies** appropriate for OT environments, including network segmentation between IT and OT domains with controlled data flows, compensating controls where traditional security measures prove infeasible, specialized threat intelligence covering OT-specific vulnerabilities and attack techniques, and incident response procedures considering both cyber and physical consequences. These requirements reflect lessons from attacks like Stuxnet, Triton, and the Ukraine power grid incidents where IT compromises led to physical impacts.

Organizations implementing CAF for OT environments must balance **security and operational requirements**, maintaining system availability while implementing security controls. The framework's outcome-focused approach proves particularly valuable here, allowing alternative controls that achieve security objectives without disrupting operations. For example, where immediate patching proves impossible, organizations might demonstrate achieved outcomes through network isolation, monitoring enhancements, and compensating controls that collectively provide equivalent risk reduction.

Official documentation and resources

The NCSC maintains comprehensive CAF documentation at **https://www.ncsc.gov.uk/collection/cyber-assessment-framework**, serving as the authoritative source for framework guidance. [National Cyber Security Centre] The main CAF v4.0 document (https://www.ncsc.gov.uk/files/NCSC-Cyber-Assessment-Framework-4.0.pdf) provides complete framework details including all principles, contributing outcomes, and IGPs with implementation guidance.

Supporting resources include the **CAF Introduction** (https://www.ncsc.gov.uk/collection/cyber-assessment-framework/introduction-to-caf) explaining framework philosophy and application, the **CAF Changelog** (https://www.ncsc.gov.uk/information/cyber-assessment-framework--caf--changelog) documenting version evolution, and various blog posts announcing updates and providing implementation insights. The August 2025 blog post (https://www.ncsc.gov.uk/blog-post/caf-v4-0-released-in-response-to-growing-threat) explains v4.0 changes responding to evolving threats.

Sector-specific guidance appears in dedicated documents like CAF for Aviation and the DGE overlay, [2T Security] while the UK Government Security portal (https://www.security.gov.uk/policy-and-guidance/introduction-to-the-cyber-assessment-framework-caf/) provides public sector implementation guidance. [2T Security] Excel assessment templates and the WebCAF portal offer practical tools for conducting assessments, with the latter providing secure, collaborative assessment capabilities for government organizations under GovAssure.

The NCSC regularly updates CAF guidance reflecting threat evolution and regulatory changes. Organizations should monitor the official collection page for updates, with CAF v5.0 development already announced to align with the upcoming Cyber Security and Resilience Bill expected in Parliament before end of 2025. [Open Access Government] [NCC Group] This future version will likely incorporate mandatory ransomware payment prohibitions, enhanced incident reporting requirements, and expanded sector coverage reflecting the broader scope of evolving regulations.