



CYBEXIS

WHITE PAPER | CRITICAL NATIONAL INFRASTRUCTURE

Raising the Bar: CNI Operators and the NCSC CAF Enhanced Profile

Key challenges and priorities for Operators of Essential Services as threat, regulation and the Cyber Assessment Framework move together

October 2026

Clarity in complexity. Confidence in every decision.

At a glance

- State actors now drive most serious attacks on UK infrastructure: the NCSC handled 200 incidents affecting CNI between January and May 2026, and attributes around three-quarters of CNI attacks to hostile states.
- CAF v4.0 (August 2025) raises expectations on threat understanding, secure software, behavioural monitoring and structured threat hunting. Enhanced Profile targets assume a capable, persistent adversary.
- The Cyber Security and Resilience Bill will widen NIS scope, introduce 24-hour initial incident notification and strengthen regulators' powers.
- The hardest part of the Enhanced Profile is rarely technology. It is scoping essential functions, evidencing outcomes in operational technology (OT) and gaining leverage over the supply chain.

Who this is for: Boards, CISOs, NIS leads and OT security managers at Operators of Essential Services (OES) and their critical suppliers.

Information correct as of October 2026. Free to share with attribution to Cybexis.

1. Why the bar is rising now

For most of the NIS Regulations' first eight years, many Operators of Essential Services treated the Cyber Assessment Framework (CAF) as an annual self-assessment: important, but periodic. That posture no longer matches the threat. The NCSC's Annual Review 2025 recorded **204 nationally significant incidents** in the twelve months to August 2025, up from 89 the year before, of which 18 were categorised as highly significant, a rise of almost 50% and the third consecutive annual increase [1].

In 2026 the picture has sharpened further. In a public lecture this year, the NCSC's chief executive disclosed that the NCSC had managed **200 cyber incidents affecting UK critical infrastructure and its supporting ecosystem between January and May 2026**, and that around three-quarters of attacks on CNI over the past year could be traced to hostile states including Russia, China and Iran. He also warned that by 2028 attackers are likely to use AI-enabled capabilities to exploit known vulnerabilities in legacy technology at scale across CNI [2].

Recent incidents show the operational reality behind those figures:

- **Pre-positioning in infrastructure.** Five Eyes advisories on the China-linked Volt Typhoon activity described actors living off the land inside energy, water and transport networks, not to steal data but to preserve the option of disruption during a future crisis.
- **Single supplier, sector-wide impact.** The 2024 ransomware attack on pathology provider Synnovis disrupted blood testing across London hospitals, and the September 2025 ransomware attack on a shared airline check-in platform caused delays at several European airports including Heathrow. In both cases the operator of the essential service was not the organisation compromised.
- **OT reached through IT.** Across sectors, the most damaging OT disruption still tends to begin in corporate IT, through stolen credentials, exposed remote access or unpatched edge devices, before moving towards control systems or forcing precautionary shutdowns.

The lesson for OES is consistent: the adversary is patient, well-resourced and comfortable exploiting dependencies the operator does not directly control. This is precisely the adversary the CAF Enhanced Profile is designed around.

2. The regulatory landscape in late 2026

CAF v4.0

The NCSC released CAF v4.0 in August 2025. It keeps the familiar structure of four objectives (A to D) and fourteen principles, but now has **41 contributing outcomes** [3][4]. Four changes matter most for operators moving towards an enhanced target:

Contributing outcome	What changed	What it means in practice
A2.b Understanding Threat (new)	Threat analysis becomes a stand-alone outcome, separate from risk management.	A documented, sector-specific view of the actors, capabilities and techniques likely to target your essential function, which visibly drives risk decisions.
A4.b Secure Software Development and Support (new)	Covers software you build and software you buy, including provenance and testing.	Supplier questionnaires, contract clauses and onboarding must address secure development, software bills of materials and vulnerability handling.
C1.f Understanding Users' and Systems' Behaviour, and Threat Intelligence (new)	Monitoring must baseline normal behaviour and use intelligence, not just signatures.	Behavioural analytics and intelligence-led detection content, including for OT protocols and engineering workstations.
C2.b Threat Hunting (rewritten)	Replaces "proactive attack discovery" with structured, repeatable hunting.	Hypothesis-driven hunts informed by A2.b, with records of scope, findings and improvements.

Table 1. CAF v4.0 changes most relevant to an Enhanced Profile (sources [3], [4]). Sector profiles are being updated to reflect the new outcomes.

CAF v4.0 also adds language on anticipating technological developments, including AI and other emerging technologies, in risk assessment (A2.a). Competent authorities are updating sector profiles and guidance to reflect the new outcomes, so operators should expect their target to be re-baselined rather than assume a previous assessment carries over.

Basic and Enhanced profiles

A CAF profile is the set of attainment levels (Not Achieved, Partially Achieved, Achieved) a regulator expects for each contributing outcome. Ofgem, for example, has set Basic and Enhanced profiles for downstream gas and electricity, with operators expected to work towards the Enhanced Profile by the end of 2027 [5]. Broadly, a Basic profile defends against common, commodity threats; an Enhanced profile assumes a **capable and persistent adversary** and expects most outcomes to be fully Achieved, including the detection, hunting, supply chain and recovery outcomes that are hardest to evidence.

The model is spreading. In June 2026 DESNZ consulted on a Tier 1 CAF profile for large electricity load controllers, built from the existing electricity sector profile, with publication envisaged in autumn 2026 [6]. The Energy Sector Cyber Security Strategy, published in May 2026, signals further work on supply chain principles through 2026 and 2027 [7].

The Cyber Security and Resilience Bill

The Cyber Security and Resilience (Network and Information Systems) Bill was introduced in November 2025, completed its Commons stages in June 2026 and is now before the House of Lords [8]. As passed by the Commons, it would bring managed service providers, data centres and large load controllers into scope, allow regulators to designate critical suppliers, and replace the current 72-hour reporting window with a two-stage regime: an **initial notification within 24 hours** and a fuller report within 72 hours [8][9]. Regulators also gain stronger investigatory and enforcement powers and a cost-recovery mechanism. Much of the detail will follow in secondary legislation, but operators should plan on the assumption that reporting, supplier oversight and evidence will all be scrutinised more closely.

Perspective

The CAF, the Bill and sector strategies are converging on the same three questions the NCSC now puts to every board: do you understand your exposure, are the fundamentals in place, and can you keep operating and recover quickly? An Enhanced Profile is simply a rigorous way of answering them with evidence.

3. Key challenges on the road to Enhanced

Scoping the essential function honestly

Many self-assessments still draw the boundary around the control system and a few supporting servers. In practice the essential function depends on identity services, remote access, historians, data links to market systems, cloud-hosted analytics, managed service providers and maintenance laptops. An Enhanced assessment that excludes those dependencies may pass on paper and fail in an incident.

Evidencing outcomes in operational technology

The CAF is outcome-based, which is helpful for OT because it does not demand IT-style controls that cannot be applied to a 20-year-old controller. But outcome-based does not mean evidence-free. Operators routinely struggle to show an accurate OT asset inventory (B4/A3), monitoring coverage of OT networks (C1), and tested recovery of engineering configurations and safety-related systems (D1). Vendor-managed assets and warranty restrictions on patching make this harder.

Turning threat intelligence into decisions

A2.b and C2.b expect a threat picture that is specific to the sector and the operator's architecture, and that changes what the operator does. Generic intelligence feeds and quarterly threat briefings rarely meet that

bar. The gap is usually the translation layer: mapping relevant actor techniques (for example, from MITRE ATT&CK for ICS) onto the operator's own attack paths, controls and detection rules.

Supply chain leverage

The new A4.b outcome and the Bill's critical supplier powers both push security obligations into contracts. Operators often discover that their most critical OT vendors and integrators are the least willing to accept new clauses, share software bills of materials or support independent testing. Long contract cycles mean the leverage often arrives years after the requirement.

Skills, resourcing and the moving target

Structured threat hunting, OT detection engineering and secure software assurance require scarce skills. At the same time, profiles are being updated to CAF v4.0 and the Bill will add reporting duties. Teams that treat each change as a separate project quickly exhaust their capacity.

4. Priorities: a pragmatic roadmap

The following priorities reflect where Enhanced Profile programmes most often stall, and where effort reduces real risk as well as regulatory exposure.

- 1. Re-baseline against CAF v4.0 and your regulator's current profile.** Map previous evidence to the 41 contributing outcomes, flag the new ones explicitly, and agree interpretation of ambiguous indicators with your competent authority early.
- 2. Define essential functions and dependencies end to end.** Produce a dependency map that includes identity, remote access, cloud services, telemetry links and every managed service provider. Treat this as the authoritative scope for both CAF and future incident reporting.
- 3. Build a threat model that drives decisions (A2.b).** Use a small number of credible scenarios, such as state pre-positioning via edge devices, ransomware in IT forcing an OT shutdown, and compromise of a remote-support supplier. Trace each to attack paths, controls and detection, and review after every significant change or intelligence update.
- 4. Fix the fundamentals that enable most intrusions.** Phishing-resistant MFA for all remote and privileged access, elimination of unmanaged remote connectivity into OT, rapid remediation of internet-facing vulnerabilities, and enforced segmentation between IT and OT with brokered, logged access.
- 5. Mature detection, then hunting (C1, C2).** Establish OT network visibility at key conduits, baseline normal behaviour, and run a quarterly cycle of hypothesis-led hunts derived from the threat model. Record each hunt so it becomes evidence.
- 6. Put security into supplier contracts (A4.b, A2.d).** Tier suppliers by impact on the essential function, then apply proportionate clauses on secure development, vulnerability disclosure, remote access, incident notification and right to audit at the next renewal.
- 7. Exercise response and recovery as if the 24-hour clock already applied (D1, D2).** Run joint IT/OT exercises that include regulator notification, supplier failure and manual operation, and test restoration of critical configurations from offline backups.
- 8. Make governance and evidence continuous (A1).** Assign an accountable owner for each contributing outcome, maintain evidence in a single repository, and report CAF attainment to the board alongside operational risk, not once a year.

Horizon	Focus	Indicative outputs
0–3 months	Baseline and scope	CAF v4.0 gap assessment; essential function dependency map; agreed interpretation points with the regulator; board-approved roadmap
3–12 months	Fundamentals and threat-informed defence	Threat model and attack paths; MFA and remote access remediation; OT visibility at key conduits; supplier tiering; first joint IT/OT exercise

Horizon	Focus	Indicative outputs
12–24 months	Enhanced capabilities	Repeatable threat hunting; behavioural detection for OT; contract clauses in place for critical suppliers; tested recovery; independent assurance against the Enhanced Profile

Table 2. An indicative phasing for operators targeting the Enhanced Profile by the end of 2027.

5. Hints for a defensible assessment

- **Write the evidence statement before the control.** For each outcome, decide what an assessor would need to see. This exposes gaps faster than reading indicators in isolation.
- **Prefer operating evidence over policy.** Logs, hunt records, exercise reports and change tickets carry far more weight than documents describing intent.
- **Be explicit about “Partially Achieved”.** A clearly reasoned partial rating with a dated improvement plan is more credible to a regulator than an optimistic “Achieved”.
- **Reuse what you already have.** ISO/IEC 27001, IEC 62443 and NIST CSF 2.0 work maps closely to many contributing outcomes. Map once and maintain a single evidence set.
- **Seek independent challenge before the regulator does.** An external review of scope and evidence quality is the most efficient way to avoid surprises at inspection.

The Enhanced Profile is demanding, but it is not arbitrary. Each contributing outcome reflects a lesson learned from real incidents against infrastructure operators. Organisations that approach it as a programme to understand and reduce their exposure, rather than a compliance return, will find that the regulatory target and operational resilience become the same thing.

About Cybexis

Cybexis is an independent UK cyber security advisory, assurance and risk management practice based in Reading. Its insights series shares practitioner perspectives on the frameworks, regulation and threats facing regulated and high-risk organisations. www.cybexis.co.uk | hello@cybexis.co.uk

This paper is for general information only and does not constitute legal or regulatory advice. Requirements, deadlines and threat activity change; always confirm current obligations with your regulator, contracting authority or certification body.

Sources and further reading

- [1] NCSC, Annual Review 2025: Incident management. <https://www.ncsc.gov.uk/collection/ncsc-annual-review-2025/chapter-01-cyber-threat-to-the-uk/incident-management>
- [2] Computer Weekly, Hostile states launched 200 attacks on UK infrastructure in five months, says NCSC chief (2026). <https://www.computerweekly.com/news/366644872/Hostile-states-launched-200-attacks-on-UK-infrastructure-in-five-months-says-NCSC-chief>
- [3] NCSC, Cyber Assessment Framework v4.0 record of changes (August 2025). https://www.ncsc.gov.uk/static-assets/documents/changelog_v4.0.pdf
- [4] NCC Group, Introducing the Cyber Assessment Framework 4.0. <https://www.nccgroup.com/introducing-the-cyber-assessment-framework-4-an-updated-tool-for-uk-cyber-resilience/>
- [5] Cydea, NCSC CAF: Basic and Enhanced profiles in the energy sector. <https://forms--cydea.netlify.app/services/ncsc-caf-cyber-assessment-framework/>
- [6] DESNZ, Large load controllers: Tier 1 CAF and associated guidance (consultation, June 2026). <https://www.gov.uk/government/consultations/large-load-controllers-tier-1-cyber-assessment-framework-and-associated-guidance>
- [7] GOV.UK, Energy sector cyber security strategy (May 2026). <https://www.gov.uk/government/publications/energy-sector-cyber-security-strategy/energy-sector-cyber-security-strategy>
- [8] UK Parliament, Cyber Security and Resilience (Network and Information Systems) Bill. <https://bills.parliament.uk/bills/4035>
- [9] J. Shelby, The UK Cyber Security and Resilience Bill: a practitioner's guide (arXiv, March 2026). <https://arxiv.org/html/2603.07861v1>