Cyberfort
Expert-led. Security Driven.

Critical Supplier Cyber Assessment

Move beyond the questionnaire. Validate what your critical suppliers actually do.

The Challenge

Compliance certifications and self-reported questionnaires provide comfort, not assurance. They measure what organisations claim to do at a point in time, not what they actually do in practice. The UK Cyber Resilience Act and NCSC Cyber Assessment Framework are raising the bar; and for organisations in regulated or critical supply chains, demonstrating genuine supplier assurance is no longer optional.

- Compliance frameworks are minimum baselines, ISO 27001 confirms roadworthiness, not actual security performance or resilience under real-world conditions
- The UK Cyber Resilience Act (2025) and NCSC Cyber Assessment Framework impose structured requirements on organisations and their critical suppliers
- Supply chain compromises are frequently undetected for weeks or months and by the time a breach is discovered, the damage is already done
- Most security teams lack the bandwidth and specialist expertise to conduct rigorous, controls based assessments of critical third parties

What We Do

Cyberfort's Critical Supplier Cyber Assessment delivers a structured, independent assessment of a defined supplier's cyber resilience, mapped against the NCSC Cyber Assessment Framework (CAF) and aligned to the requirements of the UK Cyber Resilience Act. Whether you are building on findings from a supply chain risk posture assessment, responding to a board mandate, or meeting procurement or regulatory requirements, this service provides the depth of independent assurance that self-reported compliance cannot.

The assessment covers all four CAF objectives: Managing Security Risk, Protecting Against Cyber Attack, Detecting Cyber Security Events, and Minimising the Impact of Cyber Security Incidents; delivered through a structured combination of documentary review, stakeholder interviews and technical evidence validation.

Independent Assurance

Get objective, evidence based findings that go beyond what suppliers self-report or what certifications alone can confirm

CAF Aligned Maturity Ratings

Receive a structured maturity rating across all four CAF objectives - giving you a defensible, consistent measure of supplier resilience

Regulatory Rediness

Demonstrate active supplier oversight aligned to the Cyber Resilience Act, NIS2 and DORA; reducing your own compliance exposure

Procurement Confidence

Validate supplier security claims before contract award or renewal, with independent evidence to support procurement decisions

Board Level Clarity

Translate technical assessment findings into business risk language your senior leadership and audit committee can act on

Audit Ready Evidence

Receive a structured evidence pack you can present to regulators, auditors and your own governance processes with confidence

Our Approach

Scoping & Engagement Planning
We agree the assessment scope, confirm key contacts at the supplier, and establish the engagement approach; whilst ensuring minimal disruption to your supplier relationship.

Documentary Review
We examine the supplier's security policies, risk management documentation, incident response plans and existing certifications against CAF principles and Cyber Resilience Act requirements.

Structured Stakeholder Interviews
We conduct structured interviews with supplier security, IT and leadership personnel, testing stated controls against each CAF objective.

Evidence Validation
We cross-reference claimed controls against observable technical evidence, identifying gaps between documented intent and operational reality.

Gap Analysis & Maturity Rating
We produce a maturity rating against each CAF objective and principle, identifying gaps and their potential impact on your organisation.

Reporting & Executive Briefing
We deliver a comprehensive assessment report and an executive briefing for your leadership team; providing the independent assurance your board and regulators require.

What You'll Receive

Deliverable	What it contains
CAF Aligned Assessment Report	A detailed assessment across all four CAF objectives with maturity ratings and evidence backed findings against each CAF principle
Gap Analysis & Recommendations	A prioritised gap analysis with clear, actionable recommendations for the supplier to address identified deficiencies
Cyber Resilience Act Readiness	A summary of the supplier's current readiness against key Cyber Resilience Act requirements, with a forward looking compliance roadmap
Evidence Pack	A structured evidence pack suitable for use with regulators, auditors, procurement stakeholders and your own governance processes
Executive Summary	A concise board ready briefing translating assessment findings into business risk language, for your leadership team.

Who Is This For?

- Organisations that have been identified as critical suppliers and require independent cyber resilience assurance
- Organisations seeking to ready themselves against the Cyber Resilience Act and customer supplier security mandates
- Regulated organisations (CNI, financial services, public sector, defence) with obligations to assure supplier resilience
- CISOs and IT Directors under regulatory pressure to demonstrate active supply chain oversight
- Procurement teams validating supplier security claims before contract renewal or award

Why Cyberfort?

Supply chain assessments demand more than a checklist. Cyberfort brings NCSC assured expertise, direct CAF assessment experience and deep sector knowledge across the industries where supply chain compromise carries the highest consequence. We test what suppliers actually do, not just what they say.

- ✔ NCSC Assured Cyber Security & Resilience Audit Provider, with direct experience assessing organisations against the NCSC Cyber Assessment Framework
- ✔ UK Cyber Security Council & Chartered Institute of Information Security (CIISec) certified professionals
- ✔ Methodology aligned to the EU ICT Supply Chain Security Toolbox, NCSC CAF and NIS2/DORA
- ✔ Practitioners experienced across the sectors most targeted by supply chain attacks
- ✔ Trusted by government, defence and critical national infrastructure operators

Ready to assess your critical suppliers?

Contact our team to discuss your requirements or request a scoping call:
info@cyberfortgroup.com | +44 (0)1304 814800 | cyberfortgroup.com