Cyberfort
Expert-led. Security Driven.

Supply Chain Assurance Posture Assessment

Understand your supply chain exposure before your adversaries do.

The Challenge

Most organisations rely on periodic questionnaires and point-in-time certifications to manage third-party risk. These tell you what suppliers claim, not what they actually do. As supply chain attacks grow in sophistication and regulatory expectations intensify, that gap has become a critical vulnerability.

- Only 14% of UK businesses reviewed supply chain risks posed by their immediate suppliers in the last 12 months "UK Government Cyber Security Breaches Survey 2025"
- Most organisations have limited or no visibility beyond their tier-1 suppliers, yet tier-2 and tier-3 dependencies represent significant attack surface
- Software, managed service and hardware supply chain attacks are among the most damaging and hardest to detect threat vectors organisations face
- NIS2, DORA and the UK Cyber Resilience Act are increasing regulatory scrutiny of supply chain assurance practices

What We Do

Cyberfort's Supply Chain Assurance & Posture Assessment service gives organisations a clear, structured picture of their third-party cyber risk landscape. We assess the maturity and coverage of your existing supplier assurance processes, map your supply chain for criticality, from tier-1 relationships through to tier-2 and tier-3 dependencies; and build a risk profile that translates supply chain exposure into prioritised, actionable risk based assurance plans.

Drawing on the EU ICT Supply Chain Security Toolbox, NCSC guidance and Cyberfort's own threat intelligence, we give you a structured view of not just who is in your supply chain, but what each relationship represents in terms of cyber risk and a roadmap for addressing it.

Full Ecosystem Visibility

See beyond tier-1 relationships, understand tier-2 and tier-3 dependencies that are invisible to most organisations

Prioritised Risk Exposure

Move from an unmanageable supplier list to a ranked, evidence, based view of where your real cyber risk sits

Board-Ready Output

Translate complex supply chain risk into business impact language your leadership team can act on

Regulatory Confidence

Demonstrate structured, auditable supply chain assurance aligned to NIS2, DORA and the Cyber Resilience Act

Competitive Advantage

Win regulated procurement decisions by evidencing supply chain governance that competitors cannot match

Actionable Roadmap

Leave with a clear, prioritised remediation plan; not a long list of findings with no clear next step!

Our Approach

Assurance Gap Review

Assessment of your current third party assurance framework; questionnaire coverage, certification tracking, onboarding governance and contractual security obligations.

Supply Chain Discovery & Mapping

Collaborative mapping of your supply chain across technology, data flows and service dependencies, extending visibility to tier-2 and tier-3 relationships where applicable.

Criticality Classification

Risk ranking of suppliers based on data access, operational dependency, single vendor risk and geopolitical exposure, identifying where your most significant vulnerabilities lie.

Risk Register & Remediation Roadmap

A prioritised supply chain risk register and practical remediation roadmap, with recommendations aligned to your risk appetite and regulatory obligations.

What You'll Receive

Deliverable	What it contains
Supplier Criticality Register	A tiered register of your suppliers ranked by criticality, data access, operational dependency and geopolitical exposure; covering tier-1 through tier-3 where applicable
Assurance Gap Analysis	An assessment of your current third party assurance processes questionnaire coverage, certifications, onboarding governance and contractual obligations with prioritised recommendations
Remediation Roadmap	A prioritised, practical action plan for addressing identified supply chain risks, aligned to your risk appetite and regulatory obligations
Executive Briefing Pack	A board ready summary translating supply chain risk into business impact language, suitable for senior leadership and audit committees
Executive Summary	A concise board ready briefing translating assessment findings into business risk language, for your leadership team

Who Is This For?

- Any organisation that relies on third party suppliers, from regulated industries (CNI, financial services, defence, public sector) to broader commercial supply chains; where understanding and managing cyber risk across that ecosystem is a business priority
- Organisations seeking visibility beyond tier-1 suppliers into tier-2 and tier-3 dependencies
- CISOs and IT Directors presenting supply chain risk at board level
- Procurement and risk teams strengthening third party supplier governance

Why Cyberfort?

We bring the independence, sector depth and accredited methodology that supply chain risk demands. Our practitioners work at the intersection of threat intelligence, regulatory compliance and operational security; enabling an objective picture of your supply chain exposure, not a tick-box exercise.

- ✔ 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