

Supply Chain Cyber Resilience

A QinetiQ cyber security service

From procurement to performance — assure your supply chain

Modern supply chains are vast, complex, multi-tier ecosystems of partners, subcontractors and technology providers. Few organisations can now say with confidence who delivers their services, assert the criticality of software and hardware dependencies, where data flows, or how securely information is handled. QinetiQ's **Supply Chain Cyber Resilience** service gives you that clarity — helping you map dependencies, benchmark maturity and prioritise risk across every tier.

We combine open-source intelligence (OSINT), supplier data and benchmarking against international standards to build an evidence-based picture of supplier resilience. The result is actionable insight that strengthens trust, improves oversight and protects your enterprise from disruption, data loss and reputational harm.

Key benefits

- Multi-tier cyber modelling of your entire supplier network.
- Integration of finance, procurement, contract, incident and breach data.
- Prioritisation of suppliers by risk and operational impact.
- Benchmarking of supplier maturity against peers and best practice.
- Predictive modelling to highlight weak points before they fail.
- Dashboard outputs to support enterprise and board reporting.
- Independent assessments that go beyond self-reported questionnaires.

The QinetiQ approach

SUPPLY CHAIN RESILIENCE depends on continuous insight, not one-off audits.

QinetiQ's consultants combine rapid snapshot assessments, deep-dive reviews and technology deployment to deliver lasting visibility of supply chain risk. Our approach draws on experience

supporting both government and enterprise customers, aligning analysis to recognised frameworks such as **ISO 27001**, **NIST SP 800-161, ISO 28000:2007, ISO 28001:2007 , the MOD DCPP, the NCSC/CPNI 12 Principles of Supply Chain Security and the Cloud Security Principles**.

We map supplier relationships and data flows across multiple tiers, integrating intelligence from financial systems, procurement data, cyber-incident reports and OSINT sources. Each supplier is prioritised by risk and potential impact, creating a comprehensive picture to inform a clear roadmap for targeted improvement. This can be weighted by aspects such as contract enforceability and supplier cyber improvement activities.

Our service can also assist with embedding cyber security into the planning, design and implementation of service or product procurement, working with commercial and legal specialists to develop cyber security requirements and key performance indicators (KPIs).

We are experienced in compliance assessment, audit and assurance of supplier's cyber security and advocate a partnership approach to cyber security improvement activities.

Our dashboards turn complex and often copious supplier data into meaningful intelligence — supporting procurement teams, risk managers and executives with live reporting that tracks maturity and performance over time. Predictive modelling highlights potential weak spots before they become failures, enabling proactive management and measurable resilience gains.

Why QinetiQ

- Trusted partner to defence, government and critical national infrastructure.
- Proven expertise integrating cyber, engineering and assurance.
- Experience delivering multi-tier supplier risk management for complex programmes.
- Delivered by security vetted, consultants certified under national schemes including CHECK, CREST, the UK Cyber Security Council, and NCSC.

Resilience you can see, measure and prove — across your entire supply chain.

The QinetiQ Cyber & Digital Resilience portfolio

QinetiQ's Cyber & Digital Resilience services span the full lifecycle helping organisations assess, assure and continuously improve resilience across systems, missions and enterprises.

Assess & Assure – discovery and baselining

- CHECK IT Health Check (ITHC) – Uncover vulnerabilities before adversaries do.
- Cyber Business Mapping – Map your business risks before attackers do.
- Cyber Exercising & Assurance – Realistic scenarios. Proven confidence.
- Cyber Maturity Review – Benchmark your resilience. Focus your improvements.

Respond & Improve – building resilience

- Cyber Remediation Support – Close the gaps. Strengthen your security.
- Cyber Compliance Review – Simplify compliance. Prove your readiness.
- Cyber Security Risk Assessment – Evidence-based insight. Prioritised action.

- Cyber Incident Preparedness – Be ready when it matters most.

Extend & Embed – resilience beyond technology

- Red Team Cyber Attack Simulation – The closest you'll get to a real breach — without the headlines.
- **Supply Chain Cyber Resilience** – From procurement to performance, prove your supply chain is secure.
- Cyber Security Culture Measurement – Culture is the first firewall — test its strength.

Together, these capabilities form an integrated model — from testing and assurance to recovery, improved cyber culture, readiness and resilience — giving customers confidence that their systems, people and missions can perform under pressure.

For further information: cyberenquiries@qinetiq.com
QinetiQ Ltd, Malvern Technology Centre, St Andrews Road, Malvern WR14 3PS United Kingdom
+44 (0)1252 392000 www.QinetiQ.com