

Cyber Incident Preparedness and Resilience

A QinetiQ cyber security service

Be ready when it matters most.

In a world where cyber incidents are inevitable, preparedness is the true measure of resilience. QinetiQ's Cyber Incident Preparedness service helps organisations build, test and assure their ability to respond effectively — protecting operations, resilience, reputation and stakeholder confidence.

Unlike vendors who focus only on containment, QinetiQ takes a whole-enterprise view of cyber response capability. We work across IT, legal, communications, finance and leadership teams to ensure that every decision-maker understands their role and can act effectively with confidence under pressure.

Key benefits

• Builds confidence that your organisation can respond to cyber incidents swiftly and decisively.
• Develops and exercises incident-response capability across business functions.
• Aligns to recognised frameworks including ISO 27035, NIST CSF, SANS, NCSC CAF, CREST and ENISA.
• Provides independent, quality-controlled reporting to meet regulatory and legal expectations.
• Tailors the service to your business maturity — from first-time assessments to full-scale simulations.
• Delivers assurance outputs suitable for boards, regulators and investors.

The QinetiQ approach

TRUE INCIDENT RESPONSE extends far beyond technical containment.

QinetiQ's methodology is designed to give organisations clear visibility of their readiness — technically, operationally and culturally. Each engagement typically includes:

1. **Maturity assessment** – Independent benchmarking of current response posture using ISO 27035, NIST or NCSC CAF frameworks, combined with stakeholder workshops to map decision-making structures.
2. **Scenario design and exercising** – Development of realistic, mission-relevant incident scenarios, aligned to your threat landscape and regulatory environment.
3. **Execution and evaluation** – Controlled tabletop, hybrid or live-fire simulations integrating Red, Blue and Purple teams to test detection, escalation, resilience and recovery.
4. **Post-exercise assurance reporting** – Structured analysis of performance data and decisions, presented as a comprehensive readiness report mapped to regulatory and board requirements.

Each phase is delivered by security-cleared consultants with experience in high-assurance environments — defence, national security, and critical national infrastructure.

Integrating technical rigour and executive assurance

Our approach bridges the gap between technical resilience and board accountability.
Findings are presented in two formats:

- **Technical assurance pack** – detailing playbook performance, control effectiveness, timing data, and cross-references to frameworks (e.g. ISO 27035, NIST 800-61r2, ENISA, NCSC CAF).
- **Executive summary** – a board-ready narrative outlining readiness and resilience posture, cultural strengths and areas for improvement, with clear recommendations for continuous improvement.

This dual-format reporting enables alignment between SOC operators, CISOs and executive sponsors, ensuring that technical findings translate into governance action.

Regulatory and sector alignment

QinetiQ's approach reflects expectations from the **Information Commissioner's Office (ICO)**, **NCSC**, and sector regulators including energy, telecoms, and finance.
We also align outputs to the **NCSC Cyber Assessment Framework (CAF)** and the **NIS Regulations**, enabling clients to demonstrate due diligence and operational resilience under regulatory scrutiny.

Preparedness reports are suitable for inclusion in annual assurance cycles and can form evidence packs for oversight bodies, insurers or auditors.

Deliverables

- Independent assessment of incident response maturity.
- Scenario-based exercises and data-driven evidence-based performance evaluation.
- Readiness report aligned to UK and international standards.
- Regulatory assurance mapping and compliance evidence.
- Recommendations and action plan for continuous improvement.
- Follow-up workshops to embed lessons learned.

Why QinetiQ

- Trusted partner to defence, government and critical national infrastructure.
- Proven expertise integrating cyber, engineering and assurance.
- Experience delivering hundreds of validated exercises across high-assurance environments.
- Delivered by security vetted consultants certified under national schemes including CHECK, CREST, UK CYbser Security Council and NCSC.

Cyber assurance, proven through evaluation.

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 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 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, readiness and cultural 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**