

DTP's Readiness Checklist for the UK Cyber Security & Resilience Bill 2025

New rules. Wider scope. Stronger defences.

Why this matters?

Cyber attacks are becoming more sophisticated and increasingly target supply chains. The new Bill extends security requirements to more sectors, including MSPs, and enforces higher standards of resilience and accountability.

Key Obligations (What you must do)

- ✓ **Build Security Around Risk**
Implement technical and procedural safeguards from firewalls and MFA to staff training and incident planning.
- ✓ **Lock Down Your Supply Chain**
Vet and monitor key suppliers; security is now a shared responsibility.
- ✓ **Spot & Report Fast**
Detect incidents quickly. Report to regulators within 24 hours, followed by a detailed report within 72 hours. Notify affected customers.
- ✓ **Show Your Homework**
Be audit-ready with up-to-date policies, logs and documented proof of compliance.
- ✓ **Never Stand Still**
Threats evolve, your defences must keep pace. Compliance is continuous.

How to Prepare (Steps to get ready)

- ✓ **Know Your Scope**
Identify if you're covered and track compliance deadlines.
- ✓ **Benchmark Your Security**
Align with NCSC CAF, ISO 27001, or sector-specific guidance.
- ✓ **Sharpen Incident Response**
Ensure rapid detection and 24-hour reporting readiness by practicing drills.
- ✓ **Secure Your Supply Chain**
Assess critical vendors, strengthen contracts, and monitor compliance.
- ✓ **Build a Compliance Culture**
Engage leadership, train staff, and embed security into daily operations.
- ✓ **Get Expert Help**
Bring in cybersecurity and legal specialists to close gaps quickly.

Looking to
strengthen your
cyber resilience?

The HPE Cyber Resilience Vault offers an added layer of protection against ransomware.

[Read more](#) →

[Speak to an expert](#) →