OBJECT FIRST

Checklist

UK Cyber Security and Resilience Bill: Your 6-step compliance checklist

The UK Cyber Security and Resilience Bill (CSR Bill) was introduced to Parliament on 12 November 2025, modernising and expanding the NIS Regulations 2018.

In simple terms, it's the UK government's answer to a threat landscape that has changed dramatically since 2018, as high-profile ransomware attacks, major data centre outages, and supply chain compromises targeting managed service providers have all exposed gaps in existing frameworks.

When the Bill becomes law, it will extend the scope of regulated organisations, tighten incident reporting timelines, and significantly strengthen enforcement powers—with penalties for serious breaches rising to £17 million or 4% of worldwide turnover.

This Object First CSR Bill checklist is designed to help CISOs, IT leaders, and compliance teams prepare for the Bill, navigate the compliance process, and protect your operations from cyber threats.

Please note that this checklist is intended only as a guide and is not all-inclusive. Reviewing the full Bill and associated regulatory guidance in detail is essential to ensure you understand your obligations.

1. Ascertain if you're in scope

The CSR Bill expands on NIS 2018, extending to managed service providers (MSPs), data centres above certain capacity thresholds, large load controllers to existing regulated sectors, and individual suppliers designated as 'critical' through secondary legislation.

- [ ] Confirm whether you fall under the definitions of Operators of Essential Services (OES) or Relevant Digital Service Providers (RDSPs)—see the GOV.UK CSR Bill collection page for the latest scope documentation
- [ ] Determine whether any data centre operations meet the relevant thresholds: 1 MW for shared/multitenant facilities, 10 MW for single-tenant facilities
- [ ] Assess whether you have 'Large Load Control' operations: do you remotely manage 300MW+ of electrical load?
- [ ] Review the Cyber Security and Resilience Policy Statement from DSIT to establish whether your organisation falls under the definition of an MSP
- [ ] Confirm whether you are designated as a 'critical' supplier, and establish a mechanism to stay updated with secondary legislation

2. Identify your critical suppliers

Identifying critical suppliers will be compulsory for OESs and RDSPs, and organisations should examine their **entire** supply chain for weak links:

- [ ] Map dependencies to understand which systems and services rely on each supplier
- [ ] Verify resilience—ensure backup data managed by suppliers is tamper-proof, verifiable, and recoverable under pressure
- [ ] Strengthen contracts to include incident notification obligations and defined response timelines

3. Monitor forthcoming guidance and codes of practice

Guidance from DSIT, Ofcom, and the ICO will continue to shape detailed compliance expectations, and may change quickly.

- [ ] Schedule regular reviews of your compliance posture to keep pace with codes of practice and secondary legislation
- [ ] Update policies and procedures in response to new guidance and regulatory changes

4. Review incident readiness

The CSR Bill introduces two-stage reporting, which stipulates initial notification must take place within 24 hours, followed by a full report within 72 hours:

- [ ] Establish and test customer notification mechanisms as part of regular incident response exercises
- [ ] Ensure relevant personnel understand their responsibilities and escalation pathways
- [ ] Expand incident detection to cover ransomware and prepositioning indicators—not just active service disruption
- [ ] Reference the NCSC's incident management guidance when reviewing your procedures

5. Enhance risk management and resilience

The CSR Bill requires mature, documented risk management practices across networks, systems, and supply chains:

- [ ] Ensure key policies cover risk management and cybersecurity incident response
- [ ] Deploy appropriate access controls including Multi-Factor Authentication (MFA) and Identity & Access Management (IAM)
- [ ] Validate business continuity and disaster recovery arrangements through tabletop exercises, backup restore testing, and documented recovery metrics
- [ ] Define and document Recovery Time Objectives (RTOs) for critical systems, and test regularly
- [ ] Use the NCSC Cyber Assessment Framework (CAF) as your benchmark—the expected standard for OESs and RDSPs
- [ ] If also working towards NIS2 compliance, map existing controls against CSR Bill requirements—measures for risk management, incident response, and business continuity will carry over directly

6. Implement backup storage with Absolute Immutability

The CSR Bill does not prescribe specific technologies, but its emphasis on recovery capability points clearly to the need for robust backup infrastructure. Absolute Immutability ensures that no one—not even the most privileged admin or attacker—can modify or delete your backup data. We recommend the following tactics:

- ☐ **Evaluate the benefits of S3 Object Storage**, a fully documented, open standard with native built-in immutability that enables independent penetration testing and verification
- ☐ **Ensure your backup storage delivers Zero Time to Immutability:** Backup data must be immutable the moment it is written
- ☐ **Investigate Target Storage Appliance**: A dedicated target storage appliance segments storage from backup software, and removes the risks associated with DIY self-managed backup storage during operations—particularly during setup, updates and maintenance. It requires little-to-no security expertise from a customer and shifts full responsibility to a vendor

Get more details in our Cyber Security and Resilience Bill Guide

Download our comprehensive Guide for a detailed walkthrough of the legislation and further actionable steps to build resilience that lasts.

You'll learn:

- The full scope of the CSR Bill—from which organisations are covered, to the impact of secondary legislation
- What the new requirements mean in practice, from incident reporting and supply chain obligations to enforcement powers
- How to build the cyber resilience your organisation needs—including why absolutely immutable backup storage is central to any CSR compliance strategy

Download Guide ↗

OBJECT FIRST

Simply Resilient for Veeam

Contact Us →