UK Cyber Security & Resilience Bill (CSR Bill)

What is the CSR Bill?

The Cyber Security and Resilience (Network & Information Systems) Bill (CSR Bill) is a proposed reform of the UK's Network and Information Systems (NIS) Regulations 2018, intended to strengthen the cyber resilience of critical services and digital infrastructure. While sharing common objectives with European cyber security frameworks, the UK approach places particular emphasis on outcome-based, risk-led resilience rather than prescriptive compliance.

The Bill expands regulatory scope to include additional technology-enabled and managed services, and raises expectations around operational preparedness, incident detection and response, supply-chain cyber security, and timely regulatory engagement. Supported by technical guidance from the National Cyber Security Centre (NCSC), the Bill reflects a distinctly UK model that prioritises service continuity, proportionality, and operational effectiveness, in the face of evolving cyber threats. This aligns closely with NCSC cyber resilience principles and operational good practice.

Who will be impacted?

The CSR Bill is expected to affect organisations operating within, or supporting, critical national infrastructure and essential digital services including:

- Energy and utilities
- Financial services
- Healthcare and life sciences
- Transport and logistics
- Telecommunications
- Public sector and defence
- Managed Service Providers (MSPs)
- Data centres and cloud-enabled services.

Those organisations not directly regulated may still be affected through contractual, supply-chain, and assurance obligations imposed by regulated counterparties.

Why it matters

Cyber-attacks are increasingly systemic, affecting sectors and supply chains more than ever. Existing regulations have traditionally focused on compliance, whereas the CSR Bill places greater emphasis on demonstrable operational resilience, with regulators expecting stronger cyber risk management. Many of our clients are regulated entities, who will now need to seek more from their suppliers – including CGI.

Taking NIS forwards, the CSR Bill is set to expand coverage to include managed service providers (MSPs), data centres and critical digital infrastructure, and other organisations critical to service availability. So, even organisations that aren't directly regulated will be impacted as suppliers to regulated entities.

What do we need to do?

Regulated organisations will be expected to meet enhanced expectations around cyber risk management (taking a more risk-based and outcome-driven approach to cyber resilience), improve incident detection, response, and recovery, uplift supply chain cyber security, have more robust business continuity and resilience, and meet stringent and rapid incident reporting requirements. Regulators will be given further remit to enforce, with higher levels of fines and additional powers to come via secondary legislation.

What about DORA?

Some have asked how this differs from the UK GDPR, NIS 2018, or Digital Operational Resilience Act (DORA). The CSR Bill instead focuses on service resilience, rather than (for example) data protection, having an emphasis on operational outcomes, rather than just policies. Expectations are elevated in respect of testing, exercising, and evidencing – this seeks to keep services running, rather than seeing security as a compliance exercise.

How CGI can help

CGI can support clients through:

- CSR Bill impact and applicability assessments on a consultancy basis
- Cyber resilience maturity assessments (NCSC Cyber Assessment Framework (CAF)-aligned)
- Incident response readiness and exercising
- Security Operations Centre (SOC) and resilience monitoring services
- Supplier cyber assurance and due diligence support

Why act now?

Although still awaiting Royal Assent and coming into force (likely not before 2028), organisations should begin preparing now. Many expected requirements align with NCSC guidance and emerging cyber resilience expectations. Organisations preparing early can help reduce operational disruption risk, improve regulatory readiness, strengthen supply chains, enhance incident response capabilities, and demonstrate resilience to your customers and stakeholders.

The CSR Bill moves cyber security from a compliance obligation to a core operational resilience requirement. Proactive organisations will reduce risk, regulatory exposure, and disruption.

About CGI

Insights you can act on

Founded in 1976, CGI is among the largest IT and business consulting services firms in the world.

We are insights-driven and outcomes-focused to help accelerate returns on your investments. Across hundreds of locations worldwide, we provide comprehensive, scalable and sustainable IT and business consulting services that are informed globally and delivered locally.

For more information
Visit
Cyber security

Email us at
cyber.enquiry.uk@cgi.com