

UK Cyber Security Resilience Bill

KPMG UK



KPMG. Make the Difference.

September 2026



CSRB introduced:
November 2025



House of Lords
Committee Stage:
September 2026



Royal Assent: subject to
parliamentary passage



Secondary legislation/
codes: expected
following Royal Assent



The UK's Network and Information Systems Regulations 2018 (NIS)

remain the country's only cross-sector cybersecurity legislation. The Cyber Security & Resilience Bill (CSRB) is the next major reform, designed to update and extend NIS in light of systemic digital dependencies and evolving threats.

The Government introduced the Bill on 12 November 2025. Following its passage through the House of Commons and Second Reading in the House of Lords, detailed examination begins at House of Lords Committee Stage in September 2026. Further changes may therefore be made before Royal Assent, with significant technical and sector-specific detail expected to follow.

The purpose of the CSRB is to narrow the widening gap between rising cyber risks and current defences so that essential public services and the wider economy can operate reliably. It signals a broader shift from compliance-led cybersecurity toward proactive risk management and resilience. As set out in the Government's policy statement.



By securing the digital infrastructure upon which a growing number of our businesses depend, we can deliver the stability they need to innovate and invest.

This article provides a concise, practical briefing for boards, risk leaders and technology executives on what the CSRB changes, who is likely in scope, and how to respond now – without creating a separate, duplicative programme for every jurisdiction. We outline the core additions to NIS, show how CSRB aligns with global trends (such as CER, DORA and NIS2 (European Union), SOCI (Australia), and Form 8-K and Form 10-K (USA)), amongst many others, which present an action-oriented approach so organisations can deliver measurable resilience and be ready for the detailed codes when they land.

Deeper Dive on CSRB

The CSRB updates the UK's NIS framework with tangible additions. It also situates the UK within a global pattern of cyber and operational resilience regulations that are converging on common outcomes in light of an intensifying threat landscape spanning cybercrime and state-aligned activity.

This section addresses:



Scope expansion and oversight



Incident reporting



Regulatory powers



Convergence on the same fundamentals

Scope expansion and oversight

The CSRB will expand the perimeter of regulated entities to reflect today's digital ecosystem. In addition to existing Operators of Essential Services (OES) and Relevant Digital Service Providers (RDSPs), the Bill brings the following services into scope:

- Medium and large Managed Service Providers (MSPs).
- Data centres meeting prescribed capacity thresholds, with a proposed amendment also seeking risk-based designation of smaller but systemically important facilities.
- Large load controllers meeting the applicable threshold and carrying out activities for electricity system-balancing purposes.
- Critical Suppliers designated by regulators, whose disruption could have cascading national impacts.

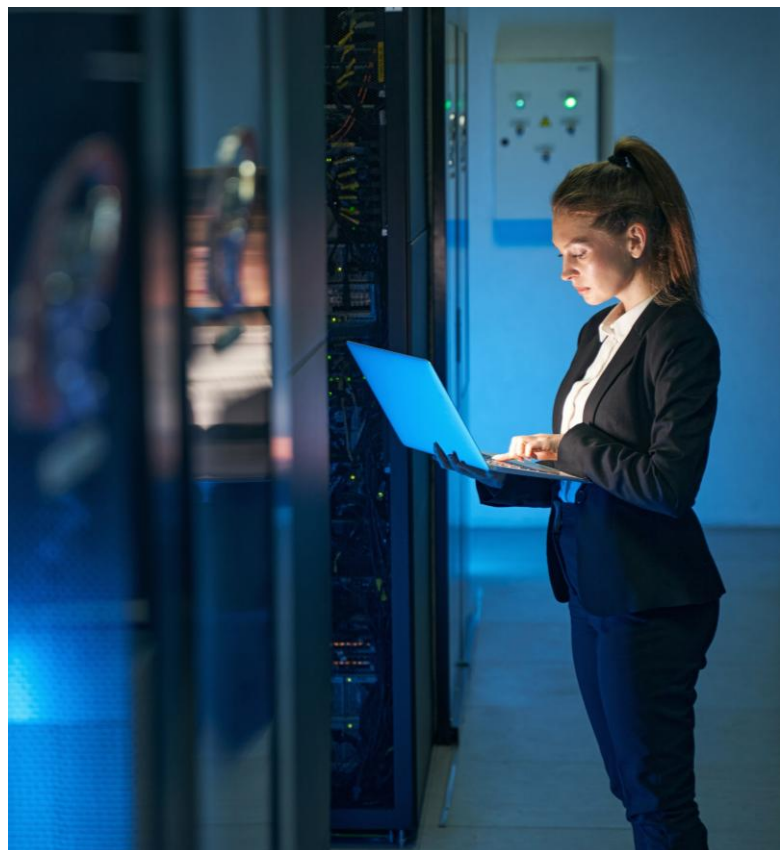
Amendments tabled for Committee Stage would potentially extend the perimeter further, including:

- Critical transport-equipment manufacturing.
- Industrial food production and processing.
- Large-scale food and essential-goods retail distribution.
- Activities in the space sector.
- Certain AI products and services, software providers and digital platforms; and
- Risk-based designation of some data centres below the prescribed capacity threshold.

Incident reporting

The Bill expands incident reporting beyond incidents that have already caused significant service disruption. As currently drafted, the regime can capture certain compromises based on their potential impact. However, an amendment tabled for Committee Stage would narrow this threshold by requiring an adverse effect to be "likely", rather than merely "capable" of occurring. A related amendment would narrow the definition of a data-centre incident by removing incidents that only could have had a significant impact. The final reporting threshold therefore remains subject to Parliamentary consideration.

Regulated entities must submit a light-touch initial notification within 24 hours, followed by a fuller report within 72 hours, with the NCSC informed in parallel to the sector regulator. In addition, customer notification duties apply in defined cases for digital services and data centres.



Regulatory Powers

The Bill equips competent authorities with a stronger, modernised toolkit to supervise and, where necessary, sanction regulated entities. This includes enhanced powers to inspect, require information and evidence, and enforce compliance, supported by updated information-sharing provisions so regulators and the NCSC can coordinate responses to incidents and systemic vulnerabilities.

The regime also enables cost recovery, allowing regulators to establish fee arrangements that fund proportionate, sustained oversight. A Statement of Strategic Priorities will provide strategic direction to regulators, with ongoing reporting to ensure delivery against those objectives.

Convergence on the same fundamentals

The CSRB does not exist in isolation. Across major economies, we see cyber and operational resilience regimes converging on a common set of five outcomes: board awareness & ability, risk assessments, business continuity, supply-chain security, and incident reporting.

While the requirements may differ, the direction of travel is the same.

Outcome	Description	CSRB	Corresponding requirements
Board awareness & ability	Active board oversight and accountable decisions on cyber risk.	Proposed amendments introduce explicit board oversight and training duties, as well as personal penalties	<ul style="list-style-type: none"> • ASPAC: CPS 234 , SOCI Act • EU: DORA, NIS2 • US: Form 10-K
Risk assessments	Proportionate, documented, risk-based programmes.	Retains NIS expectation of “appropriate and proportionate” security and resilience measures.	<ul style="list-style-type: none"> • ASPAC: CPS 234 , SOCI Act • EU: CER. DORA, NIS2 • US: Form 10-K
Business continuity	Continuity proven by testing and exercising, not policy alone.	Aimed at protecting the continuity of services critical to daily life.	<ul style="list-style-type: none"> • ASPAC: CPS 234 , SOCI Act • EU: CER. DORA, NIS2 • US: Form 10-K
Supply-chain security	Manage systemic risk in critical providers and dependencies.	Widens scope to MSPs and data centres and enables Critical Supplier designation.	<ul style="list-style-type: none"> • ASPAC: CPS 234 , SOCI Act • EU: CER. DORA, NIS2 • US: Form 10-K
Incident reporting	Faster notification and clearer external communications.	Requires reporting to regulator and NCSC, with targeted customer notices for digital services and data centres.	<ul style="list-style-type: none"> • ASPAC: CPS 234 , SOCI Act • EU: CER. DORA, NIS2 • US: Form 8-K

Key Challenges

As the CSRB broadens its scope, accelerates deadlines, and intensifies regulatory oversight, organisations are confronted with a heightened array of challenges. We have identified and highlighted the key difficulties companies may encounter when aligning with the new CSRB requirements.

These challenges can be grouped into three main categories:



01. Governance challenges

1. Understanding scope and applicability

The regulatory perimeter is broadened beyond the traditional OES/RDSPs to include MSPs, certain data centres, large load controllers, and designated critical suppliers, including those established outside the UK but offering services into it.

Multi-entity and cross-border operating models further complicate scoping, because a single digital service can bring several UK and non-UK entities into scope through operational or contractual links.

2. Managing the increased workload

The CSRB's accelerated notification timelines and expanded regulatory touchpoints compress activities that organisations typically spread across days or weeks. Legal, communications, operations and cyber teams must produce coordinated outputs within 24 and 72 hours, at a time when investigative facts may still be emerging.

Executing these obligations across time zones, third parties and sector authorities creates a sustained operational burden.

3. Managing budgets

Running parallel initiatives for CSRB, NIS2, SOCI Act, and other regulations rapidly inflates costs because many controls are substantively similar but may be maintained in different formats and cadences.

In addition, the CSRB's cost-recovery provisions introduce ongoing supervisory fees, which regulators can levy on in-scope entities to fund the costs of overseeing and enforcing the Bill. Each regulator will set its own fee regime, which makes duplication financially unsustainable.

4. Establishing executive ownership and evidence of oversight

Organisations must move beyond general C-suite sponsorship towards identifiable ownership, informed challenge and evidence of key decisions. Proposed amendments would introduce explicit board oversight and training duties and could expose senior executives to penalties in cases involving consent, connivance or neglect. Even if these amendments are not adopted in their present form, organisations should maintain clear decision records, escalation routes and periodic assurance over security and resilience risks.

5. Transitioning from one-off project to BAU

The Bill's evolving codes of practice and enhanced regulator powers will shape expectations over time. As a result, exercising, supplier oversight, metrics, and evidence refreshes must become regular activities rather than one-off tasks.

Sustaining compliance and resilience requires an operating model that tracks and adapts to regulatory changes. Many organisations are initially mobilised around deadlines and deliverables, making it difficult to pivot to this model.

02. Risk management challenges

1. Security operations

The CSRB places emphasis on early detection and rapid incident reporting, raising expectations around security operations maturity. Organisations must ensure that monitoring covers the full range of in-scope services, including dependencies and designated critical suppliers.

Any shortcomings can hinder the ability to meet the crucial 24-hour notification window, potentially increasing regulatory risk.

2. OT security

For organisations operating critical infrastructure or large load controllers, OT environments introduce unique risks not always addressed in traditional IT-focused programmes. This area has historically received less attention and resources than its IT counterpart but is now central to meeting regulatory expectations.

Legacy assets, limited patchability, segmented architectures, and safety-critical constraints make it harder to implement safety measures that are both suitable and effective. With the CSRB expanding its reach to include more industrial and energy sectors, it is essential that OT considerations are fully integrated into organisational security strategies.

3. Third-party risk management

The CSRB explicitly extends regulatory attention into the supply chain, including the ability to designate "Critical Suppliers". This increases the burden on organisations to evidence how they assess supplier dependencies and manage shared risks. Supplier portfolios are often dispersed across multiple business units and legacy procurement processes, making it difficult to apply a single, risk-based method for determining criticality.

In addition, many older contracts lack the clauses needed to require enhanced security controls, evidence sharing or participation in joint resilience activities. As a result, organisations can face delays and commercial resistance when attempting to uplift supplier obligations.

03. Technical challenges

1. Penetration testing

The CSRB has not yet mandated specific testing methods; however, technical requirements are expected to be set later via secondary legislation, codes of practice, and sector-specific guidance.

There is a growing regulatory expectation for organisations to adopt threat-led and risk-based testing for critical services, aligning with broader trends in other resilience frameworks. Organisations need to ensure their testing activities cover all in-scope entities, including digital platforms and externally managed environments.

2. Legacy constraints

Older platforms often cannot support modern security controls, increasing the cost and complexity of meeting CSRB expectations. Organisations must balance remediation, compensating controls and strategic modernisation.

3. Asset visibility

Many organisations still lack a consolidated view of assets across IT, OT, cloud and service providers. The CSRB's focus on understanding in-scope services highlights the importance of maintaining accurate inventories and configuration data.

4. Logging and monitoring

Accelerated reporting timelines demand faster access to high-quality telemetry. Gaps in logging and monitoring or inconsistent retention policies can hinder forensic readiness and make it harder to meet notification obligations.

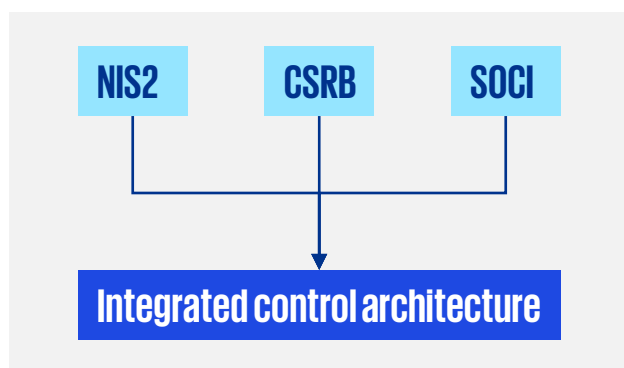


Confronting these challenges

As organisations move beyond establishing foundational controls, a proactive approach to regulatory readiness is vital. This means not only preparing for known requirements, but also embedding agility into compliance programmes to quickly align with future updates.

Build once, comply for many

Our approach advocates the creation of a single, integrated control architecture that utilises the convergence themes present in various regulatory frameworks, including CSRB, NIS2 and SOCI. By mapping controls across these regimes, organisations can avoid redundancy, streamline compliance, and adapt efficiently to differing reporting requirements.



Plan for iteration

The Bill continues to evolve through the Parliamentary process, with Committee Stage amendments highlighting that the final regulatory perimeter, incident thresholds, governance expectations and intervention powers may change before Royal Assent. Organisations should monitor developments closely and maintain a structured change log to assess legislative changes, track implementation decisions and adapt efficiently as requirements become clearer.

Treat suppliers as an integral part of cyber resilience

Suppliers should be considered as core elements of your organisation's security environment, rather than external entities. Building a critical supplier watchlist, revising and uplifting contractual standards, and conducting joint exercises and reporting drills are essential steps for maintaining robust oversight.

Organisations should also map material technology vendors and identify credible exit or substitution options, particularly where products support essential services or create concentrated dependencies.

NB: Technical details will follow through secondary legislation and codes after Royal Assent, with further government consultation expected in 2026. Until competent authorities publish their approaches however, organisations face uncertainty over how requirements will be interpreted, evidenced, and supervised.

It is important to develop an iterative programme, delivering "no-regrets" capabilities now, and maintaining a regulatory change log so you can adopt final codes with minimal rework.

KPMG Case Study: Managing Increasing Compliance Efforts

On a daily basis we see increased scrutiny for regulatory compliance across various products and jurisdictions.

As well as supporting our clients in implementing key requirements, we also support clients in audit readiness programmes, designed to ingest new regulatory matters, breaking them down into legal interpretations, and then testing those controls for completeness on both a design and implementation basis.

We see common hot spots for non-compliance across our clients and our audit readiness programmes have helped to identify these prior to regulatory implementation and comfortably ahead of any regulatory audits. This has allowed our clients to proactively produce remediation plans or strategic positions ahead of an audit, increasing their compliance structure whilst also allowing them to prepare in advance of a high state audit.

With the increased regulatory landscape, we are seeing further regulations being applicable to our clients including India's NPCI UPI Information Security Compliance Framework, EU AI Act, South Korea's BCDA and more. KPMG has provided expertise in these regulatory matters including on the ground support of regulatory audits, managing client SME's and producing and delivering audit responses.



How KPMG can help

The UK CSRB represents a deliberate step-change in the UK's cross-sector cyber regime: it widens the perimeter, accelerates incident visibility, and equips regulators to steer and scrutinise outcomes more effectively.

MVC Approach: protecting what matters most.

A Minimum Viable Company (MVC) is the minimum set of core business services required to maintain continuity during a major disruption. Defining MVC upfront provides a business-led basis for prioritising resilience investment and making faster, clearer recovery decisions.

KPMG's holistic approach focuses on what is essential for businesses to continue operating.

The CSRB is centred on sustaining essential services that society, the economy, and public safety rely on. An MVC turns this intent into a practical operating model by specifying which services must be preserved and the minimum capabilities required to do so.

Defined in advance, this enables organisations to continue delivering critical business even when an incident or disruption happens.

For more information on why focusing on critical functions matters, see KPMG's policy statement on the CSRB [here](#).

In conjunction with MVC, KPMG has extensive experience in delivering resilience programmes across multiple jurisdictions. Our teams operate end-to-end, from scoping and dependency mapping through to full-scale implementation.

As a trusted partner, we offer the following services:

01. Risk & Readiness assessments

We identify in-scope entities, map dependencies, and perform risk & readiness assessments to ensure comprehensive coverage.

02. Incident notification and response

Our experts design, exercise and refine notification runbooks through realistic tabletop exercises, preparing organisations for effective incident management.



03. Supply-chain uplift

We strengthen third party controls and conduct thorough supply chain assessments to enhance overall resilience.

04. OT Security Improvement

For organisations with operational or industrial environments, we uplift OT security in line with standards like IEC 62443. This delivers measurable improvements without disrupting essential operations.

05. IT/OT Asset Management

We create a consolidated view of assets across IT, OT, cloud, and managed services. By aligning telemetry to improve detection and reporting readiness, we enable traceability that supports regulatory compliance and forensic capabilities.

06. Awareness Campaigns

We run executive briefings and role-based workshops to embed accountable decision-making on cyber risk. We also deliver targeted training for operations teams focused on practical controls and improvements.

07. Transition to BAU Model

We deliver these cyber and operational resilience programmes from initial mobilisation to ongoing compliance by establishing governance structures and assurance cycles. We embed sustainable operating models that treat regulatory expectations as a continuing obligation rather than a one-off project.



Author



Hamish Wishart

hamish.wishart@kpmg.co.uk

Your contacts



Janina Herrmann

janina.herrmann@kpmg.co.uk



Elizabeth Huthman

elizabeth.huthman@kpmg.co.uk



kpmg.com/uk

Some or all of the services described herein may not be permissible for KPMG audited entities and their affiliates or related entities.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.

Document Classification: KPMG Public

CREATE: CRT166156A | September 2026