

PERSPECTIVE · OCTOBER 2026

UK CSRB and its potential impact on regulated firms such as *banks and insurers*

Cyber Security and Resilience (Network and Information Systems) Bill
Status as at 6 October 2026. The Bill is still before Parliament.

Executive Summary and Recommendations:

- The government expects Royal Assent around spring 2027, subject to the remaining parliamentary stages, and the main duties in force from 2028 at the earliest. The duties cannot be enforced until the regulations that commence them are made, so enforcement by the Information Commission (managed service and cloud providers), Ofcom (data centres) and the other regulators is **not realistic before 2028-29**.
- This gives in-scope service providers, and suppliers that could be designated as critical, **time to improve resilience and incident reporting before the duties apply, and to avoid regulatory fines**.
- In the interim, regulated firms such as banks and insurers, as business customers of these providers, **rely on Prudential Regulation Authority (PRA) SS2/21, Financial Conduct Authority (FCA) FG26/4 and their contracts**. The PRA and FCA material third party register, required **from 18 March 2027**, covers many of the same suppliers well before the CSRB is enforced.
- Insurers that write corporate policies for these providers should **use the 2027 renewal season to review underwriting guidelines and pricing**, starting with three gaps: notice conditions that do not fit a 24-hour statutory clock, one supplier event reaching several towers and its customers' policies, and data centre damage that falls between property and cyber cover.

1. Banks and insurers will feel the CSRB through their suppliers

The Bill does not regulate banking or insurance. Its effect on a bank or insurer comes through the managed service providers, cloud providers and data centres it buys from. PRA and FCA operational-resilience and outsourcing rules continue on their own terms, and a supplier's notice under the Bill becomes an input to those duties.

Suppliers take on new duties. Medium and large managed service providers must register with the Information Commission, apply proportionate security measures and report significant incidents. Data centres above the thresholds become operators of essential services, regulated by Ofcom. Cloud providers, already in scope, face tighter reporting rules.

Incident reporting becomes faster and wider. A regulated supplier must notify its regulator, with a copy to the National Cyber Security Centre, within 24 hours of becoming aware of a significant incident and send a full report within 72 hours. Reportable incidents include events capable of a significant impact, such as ransomware and pre-positioning, whether or not the impact has occurred. After the full report, the supplier must, as soon as reasonably practicable, notify the UK customers likely to be adversely affected, explaining the nature of the incident and why the customer is likely to be affected.

Customers will receive that notice before the facts are complete. A bank or insurer should route it into its own incident and outsourcing processes.

National-security directions add a risk outside commercial control. The Secretary of State can direct a regulated supplier to stop using, or to remove, specified goods or services. A direction can interrupt a hosting, claims or payments stack with little commercial warning.

Contracts need three additions to existing SS2/21 terms. The statutory clock gives the customer notice only after the 72-hour full report, so a supplier to an important business service should be required to notify earlier. A national-security direction falls outside ordinary termination and force majeure events, so exit and substitution rights should name it expressly. Registration under the CSRB and flow-down to subcontractors become evidence requests at onboarding and renewal.

Start with the register the firm must build anyway. From 18 March 2027 banks and insurers report material third party arrangements to the PRA and FCA, including an annual register (PS7/26, PS26/2 and FG26/4). That register covers many of the suppliers the CSRB will regulate. Marking which of them are managed service providers, cloud providers or in-threshold data centres turns the PRA and FCA work into the firm's CSRB map, a year or more before the CSRB is enforced.

2. Insurers that cover in-scope firms face the sharper change

The insured population is changing. Newly exposed insureds are medium and large managed service providers, data centres above the thresholds, large load controllers and any designated critical supplier. Existing operators of essential services face tighter reporting rules and higher penalty bands.

Current wordings will sit awkwardly beside the new duties. A notice condition framed only as “as soon as practicable”, or an incident definition that requires actual business interruption or data loss, does not fit a 24-hour statutory notification and a wider class of reportable event. Insurers should expect earlier notifications, and more forensic and customer-notification costs.

Fines and related costs need an explicit position. Regulatory penalties raise a separate question of insurability under English law, and most cyber forms already exclude fines that are uninsurable by law. FCA and PRA rules bar regulated firms, insurers included, from insuring a financial penalty imposed by either regulator (FCA GEN 6.1.5 R; PRA General Provisions 7.3), although the FCA allows cover for defence costs. No rule or court decision settles whether NIS penalties can be insured, and we expect underwriters to keep them outside cover for at least the next few years. Defence costs, investigation costs and the customer-notification exercise still need a stated position.

One supplier incident can trigger many claims. For a managed service provider, a failure of the security duty or of the duty to notify customers can arrive both as a regulatory penalty and as a customer claim in contract or negligence. The same incident can reach the supplier’s cyber tower, its professional-indemnity tower, and the cyber and interruption policies of its customers. Aggregation wording therefore matters.

Some losses will fall between policies. At a data centre, hardware damage from a compromised cooling or power system can fall between a property policy that requires an insured physical peril and a cyber policy that excludes physical damage. Underwriters should decide which policy responds to that loss, and say so in both wordings, before a claim tests it. A direction to isolate a system or drop a supplier can stop operations without a conventional insured event.

Proposal forms should establish scope. They should ask whether the insured is an operator of essential services, a relevant managed service provider, an in-threshold data centre or a designated critical supplier, and whether it can notify a regulator within 24 hours.

3. Three questions for the Board this quarter

Banks, insurers and other regulated firms: Which of our managed service providers, cloud providers and data centres will the CSRB regulate, and which of them support an important business service? Align incident playbooks with the supplier’s statutory clock: regulator notice within 24 hours, full report within 72 hours, and customer notice after that. For suppliers that support an important business service, contract for earlier notice.

Insurers covering in-scope service providers: Do our cyber and professional-indemnity wordings respond to a 24-hour notification duty, a national-security direction and an aggregated supplier event? Most of these policies renew annually. Use the 2027 and 2028 renewals to add the scope questions, set positions on fines, notification and aggregation, and reflect the change in pricing ahead of the expected enforcement window.

In-scope service providers and suppliers that could be designated: Could we evidence today the security measures and incident reporting the regulator will expect from 2028? Make the improvements now and build the cost of compliance and insurance into pricing.

4. The Bill in brief

Status: The Bill is a government bill from the Department for Science, Innovation and Technology, in the charge of Liz Kendall in the Commons and Baroness Lloyd of Effra in the Lords. It was introduced on 12 November 2025, completed the Commons on 16 June 2026 and Lords committee on 7 September 2026. The current text is HL Bill 49, and Lords report stage is scheduled for 26 October 2026. Commentators have put Royal Assent at late 2026 or spring 2027; a June 2026 government consultation (Department for Energy Security and Net Zero) pointed to spring 2027. Some provisions commence on Royal Assent, some two months later, and the rest on dates set by regulations.

Scope: The Bill amends the Network and Information Systems Regulations 2018. The persons who can be enforced against are:

- Operators of essential services in energy, transport, health, drinking water and digital infrastructure.
- Operators of data centre services, at a rated IT load of 1 MW or more, or 10 MW where the service is provided on an enterprise basis.
- Large load controllers, with potential electrical control of 300 MW or more.
- Relevant digital service providers: online marketplaces, online search engines and cloud computing services.
- Relevant managed service providers.
- Suppliers designated as critical suppliers.

Managed services: A managed service is the ongoing management of a customer's information technology systems under a contract, where the provider connects to or otherwise obtains access to the network and information systems the customer relies on, on site or remotely. A relevant managed service provider provides a managed service in the United Kingdom, whether or not established here, and is not a micro or small enterprise under Commission Recommendation 2003/361/EC (fewer than 50 staff, and annual turnover or balance sheet

total of EUR 10 million or less). A person under public authority oversight is also outside this category unless more than half of its income is commercial. Relevant digital service providers keep the same size exemption.

Banks and insurers: Banking and financial market infrastructure were left out of the 2018 Regulations because the Bank of England and the FCA already set requirements for those sectors, and the Bill does not add banking or insurance. A bank or insurer is regulated only if a particular activity falls inside a category above, such as a data centre at or above the threshold, a relevant managed service, or designation as a critical supplier.

Penalties and directions: A failure of the security, incident-reporting or customer-notification duties carries a maximum penalty of the greater of £17 million and 4 per cent of worldwide turnover; an administrative failure, such as registration, carries the greater of £10 million and 2 per cent. The Secretary of State may give a direction to a regulated person, including a designated critical supplier, where a threat to network and information systems gives rise to a risk to national security and the direction is necessary and proportionate. A breach can attract up to £17 million or, where regulations are in force, the greater of £17 million and 10 per cent of turnover, with daily penalties of up to £100,000.

Critical suppliers: Designation is the supply-chain route; a third or fourth party is otherwise outside the regime. The regulator can designate a supplier that provides goods or services directly to an operator of essential services, a relevant digital service provider or a relevant managed service provider, where an incident on the supplier's systems could disrupt that service and the disruption is likely to have a significant impact on the economy or day-to-day functioning of society in the United Kingdom or part of it. The regulator must consider alternative sources of supply and whether the risk can be managed by other means. Small and micro firms can be designated. The supplier has a right to make representations and to appeal to the First-tier Tribunal and must notify the regulator if it believes it no longer meets the conditions. The factsheets illustrate the power with the June 2024 attack on Synnovis, a pathology provider to the NHS. No names have been published; designation waits on secondary legislation, and the government states that duties on critical suppliers will not be more stringent than those on operators of essential services and on digital and managed service providers.

We will be happy to bring the benefit of our experience and regulatory expertise to stakeholders directly and indirectly affected by the CSRB and the other regulations cited in this paper.

Santosh Pandit · Board and CxO Advisor · Founder, BeatQuantum Limited

BeatQuantum.com | SantoshPandit.com | contact@santoshpandit.com

References

1. UK Parliament, Cyber Security and Resilience (Network and Information Systems) Bill, stages and documents. <https://bills.parliament.uk/bills/4035>
2. HL Bill 49, as amended in Grand Committee, 7 September 2026. <https://bills.parliament.uk/publications/67673/documents/8744>
3. Explanatory Notes to HL Bill 32, June 2026. <https://publications.parliament.uk/pa/bills/lbill/59-02/032/en/5902032en01.htm>
4. Department for Science, Innovation and Technology, Bill factsheets, updated 30 June 2026. <https://www.gov.uk/government/publications/cyber-security-and-resilience-network-and-information-systems-bill-factsheets>
5. Department for Energy Security and Net Zero, Large Load Controllers: Tier 1 Cyber Assessment Framework and associated guidance, consultation, 23 June 2026. <https://www.gov.uk/government/consultations/large-load-controllers-tier-1-cyber-assessment-framework-and-associated-guidance>
6. PRA, SS2/21 Outsourcing and third party risk management. <https://www.bankofengland.co.uk/prudential-regulation/publication/2021/march/outsourcing-and-third-party-risk-management-ss>
7. FCA, FG26/4 Material Third Party Reporting, March 2026. <https://www.fca.org.uk/publication/finalised-guidance/fg26-4.pdf>
8. FCA Handbook, GEN 6.1 Payment of financial penalties. <https://www.handbook.fca.org.uk/handbook/GEN/6/1.html>
9. PRA Rulebook, General Provisions, Chapter 7 Insurance Against Financial Penalties. <https://www.prarulebook.co.uk/prarules/general-provisions/7-insurance-against-financial-penalties/01-05-2024?p=1>