THE CYBER SECURITY & RESILIENCE BILL

WHAT IT MEANS AND HOW WRANGU AND SERVICENOW CAN HELP

Date: 20 November 2025

Audience:

CISOs and Risk Leaders across UK Government, CNI and regulated services, Senior Civil Servants.

The Bill brings more organisations within scope and introduces tougher penalties, with powers for Government to intervene where needed

Acting now ensures compliance and delivers stronger resilience, greater efficiency, and improved stakeholder transparency – turning compliance into a strategic advantage.

Wrangu and ServiceNow enable rapid deployment of an integrated control environment to stay ahead of regulatory demands and evolving threats.

EXECUTIVE CONTEXT

The Government's Cyber Security and Resilience (Network and Information Systems) Bill, introduced to Parliament on 12 November 2025, represents the UK's most substantive refresh of the NIS framework since 2018. Proposed new laws are designed to strengthen cyber defences for essential public services like healthcare, drinking water providers, transportation,and energy, with clearer expectations of executive accountability and stronger powers for the Government and regulators to test, direct and, where necessary, sanction.

Assuming a smooth passage, secondary legislation and sector guidance will follow through 2026, and it is prudent to plan on the basis that the regime will bite from mid-year.

For government, critical infrastructure and other regulated services, the bill signals a broader shift in what "good" looks like. It means tougher cyber-resilience expectations, faster incident reporting, stronger oversight and accountability, and a higher bar for security across both organisations and their supply chains.

POLITICAL AND TECHNOLOGY CONTEXT

Ministers have signalled an appetite to modernise critical digital infrastructure even within a deregulatory agenda elsewhere, and recent high-profile incidents across the economy have hardened public expectations of both service continuity and accountability. Artificial intelligence, meanwhile, is changing the capabilities available to both attackers and defenders; a platform that can incorporate automated detection, response and control monitoring while maintaining clear human accountability will allow organisations to adopt new technology with confidence rather than caution.

WHAT THE BILL DOES (IN SUBSTANCE)

At its core, the Bill widens the net. In addition to traditional essential service operators, it brings data centres, managed service providers, and designated critical suppliers within scope, alongside certain actors in the energy system. The Government's intent is straightforward: if an organisation's failure could materially disrupt essential services or the wider economy, it should meet a defined bar for cyber resilience and be capable of proving it.

Complementing this, the Bill tightens incident reporting, expecting an initial notification to competent authorities and the NCSC within twenty-four hours and a fuller account within seventy-two hours, with providers notifying affected customers where applicable. Regulators are equipped with enhanced information gathering and direction powers and the ability to recover costs of oversight. Penalties rise to the greater of seventeen million pounds or four per cent of global turnover for serious failures, meaning large organisations could face fines on a scale comparable to the operational disruption caused by a major incident. It is a clear signal that weak governance and slow or inaccurate reporting now carry significant financial and reputational risk.

IMPLICATIONS FOR PUBLIC BODIES, CNI AND MAJOR CORPORATES

As government strengthens requirements for CNI in response to the changing threat and technological landscape, wider public sector leaders should also be taking steps to strengthen organisational security and resilience - this is ever more important as the digital transformation agenda builds pace. For example, boards will need clear sight of cyber risk and control health, with service owners able to trace essential functions through to the applications, physical and cloud locations, including data centre regions, and suppliers on which they depend.

Managed service providers should assume a regulated posture. Privileged access must be tightly governed. Incident playbooks must contemplate customer notification duties. Assurance evidence must be readily available to clients and regulators alike.

If you rely on suppliers who are designated critical or operate out of in scope data centres, they will be drawn into faster reporting cycles and greater scrutiny of third-party controls. Across the board, the cultural implication is as important as the technical one: resilience is now an auditable business discipline, not an engineering aspiration.

RANSOMWARE POSTURE AND STANDARDS ANCHOR

Although the Bill is not a ransomware instrument per se, it sits alongside a tougher public sector posture, with the Home Office considering legislation including measures to ban ransomware payments for owners and operators of regulated-critical national infrastructure and the public sector. For departments, NHS bodies and CNI operators, this raises the bar for preparedness: resilient backups, tested restoration, sanctions checks and communications discipline must be in place before a crisis, not assembled in the heat of it.

More broadly, the regime points to the NCSC's Cyber Assessment Framework as the yardstick for what good looks like, and its requirements are expected to be put on a stronger footing. In practical terms, organisations will be expected to show mature governance and risk management, robust identity and access controls, credible monitoring and detection, well rehearsed response and recovery, and a cycle of learning, each evidenced in a way a regulator can examine.

HOW TO RESPOND NOW

The immediate question is how to react while the bill progresses and secondary rules are drafted. The sensible approach is to behave as if the obligations already exist, and to concentrate on three themes: evidence, speed, and dependency clarity. Evidence means aligning governance, risk, and controls to Cyber Assessment Framework outcomes and being able to show, not merely assert, that they work: who owns each control, how it is tested, what was found, and what was fixed.

Speed means industrialising incident command so that detection, triage, legal determinations and executive approvals are orchestrated and time stamped, enabling accurate submissions within twenty-four and seventy-two hours and, where required, prompt customer notifications.

Dependency clarity means mapping essential services to the systems, data centres, regions and suppliers that underpin them, including privileged access by managed service providers, so that single points of failure, failover routes and communications paths are unambiguous.

A MODERN CONTROL ENVIRONMENT

To do this at scale, departments need more than individual tools. They need an integrated control environment that gives leaders a single view of risk, incidents, suppliers and AI in terms that make sense for service delivery. In practical terms that means being able to answer three questions at any point.

- Are we facing material cyber activity or incidents that threaten service delivery?
- Are our critical suppliers and managed service providers being managed to an acceptable level of risk?
- Where is AI deployed in our organisation and is it operating within agreed policy and risk tolerances?

The answer does not need a new system of record. It needs a unifying layer across existing processes, so that AI, Security Incident Response, Security Operations, Vulnerability Response, Integrated Risk Management and Third-Party risk capabilities work over a common data model. In a mature state, the same information that drives operational dashboards also feeds audit and risk committees, executive boards and Accounting Officers, so that scrutiny is based on evidence and record rather than subjective narratives.

HOW WRANGU AND SERVICENOW CAN HELP

Wrangu applies the power of the ServiceNow AI Platform in the context of UK public service.

In governance, risk and compliance, ServiceNow Integrated Risk Management capabilities allow departments and regulated entities to model objectives and principles as first class objects, link them to specific risks and controls, and attach evidence in one system of record. This produces regulator ready reporting without the evidence chase that so often undermines credibility.

In security operations, ServiceNow Security Incident Response and Major Incident Management codify the twenty-four and seventy-two hour reporting journey. Alerts are triaged, forensic notes and legal assessments are captured, decision points are recorded with approvals, and initial and full reports can be generated consistently and quickly. Where providers must notify customers, those communications can be orchestrated as part of the same workflow, avoiding duplication, error and delay.

ServiceNow Third-Party Risk Management catalogues suppliers and managed service providers, manages attestations and controls testing, tracks breach notification obligations, and surfaces residual risk to Boards and Audit and Risk Committees. In business continuity, the tooling helps run impact analyses, plan and rehearse recovery, and capture lessons learned, reinforcing a no ransom posture with practical recovery discipline. The ServiceNow AI Platform provides a single pane of glass that connects intelligence to execution across every corner of business, integrating with any cloud, any model, and any data source to orchestrate how work flows across the enterprise. Departments can stand up an initial version in days and weeks and then strengthen it release by release, so that resilience, evidence and reporting stay ahead of policy, regulatory demands and the evolving threat landscape rather than repeatedly trying to catch up. A phased implementation does not dilute accountability. It allows continuous improvement without waiting for a single large programme.

BOTTOM LINE

Assurance is becoming a statutory duty and evidence the currency in which it is measured. Organisations that start now, by aligning to the Cyber Assessment Framework, industrialising incident reporting, mapping their dependencies and tightening supplier governance, will not only meet the letter of the law when it arrives; they will be materially more resilient, more efficient and more transparent to their stakeholders. ServiceNow provides the platform to make that shift real, Wrangu accelerates delivery, and your teams retain the governance. Compliance, in this model, is not a cost centre; it is the visible expression of a system that works.