REPORT

How to Prepare for the UK Cyber Security and Resilience Bill in 2025

Preparing for Supply Chain Compliance Under the UK Cyber Security and Resilience Bill

SecurityScorecard

Executive Summary

Cyberattacks on the UK's critical infrastructure have become persistent, systemic, and increasingly driven by supply chain vulnerabilities. Disruptions to essential services and breaches across government departments highlight an urgent need: The UK's cyber regulatory framework must evolve to properly manage escalating risk and thwart damaging cyberattacks.

Recent incidents have left thousands of patients without access to timely care and prompted renewed scrutiny across the UK as Parliament prepares to overhaul cyber regulations governing critical national infrastructure.

To safeguard essential services and limit economic disruption, organisations will soon need to comply with the Cyber Security and Resilience Bill. Announced in the July 2024 King's Speech, the Bill would update the UK's regulatory framework to address crucial gaps in cyber resilience, with a particular focus on staying one step ahead of threat actors and managing risk from supply-chain dependencies.

The Supply-Chain Element

SecurityScorecard's 2025 Global Third-Party Breach Report shows that more than one in three data breaches now originate with third parties. Threat actors constantly revise their attack playbooks to find the path of least resistance, and iIncreasingly, that path runs through organisations' supply chains.

Despite existing frameworks, attackers continue to exploit unseen weaknesses in UK supplier ecosystems, revealing a fundamental visibility gap. A rising cadence of these kinds of attacks has forced regulatory change.

Beyond the European Approach

Many UK organisations follow European cyber directives when operating within the EU, such as the Network and Information Systems Directive 2 (NIS2), in force since October 2024.

Still, the UK government acknowledges current laws have not kept pace with rapid technological change and that organisations in the UK need a new direction, with proactive monitoring and information-sharing.

As third-party and cloud ecosystems continue to expand, the government is shaping a framework that evolves alongside adversary tactics, strengthening both oversight and national cyber posture.

Here is what organisations can do to keep pace with changes expected from the Bill, including preparing for reporting obligations and strengthening supply chain oversight. This report covers:

- **The strategic drivers behind the Bill,** including recent UK-based supply chain breaches, global attack trends, and threat actor tactics.
- **A side-by-side look at the UK Bill and NIS2** as well as supply chain assessment mandates.
- **A detailed breakdown of anticipated provisions,** such as the designation of critical suppliers, inclusion of Managed Service Providers (MSPs) and data centres, and expanded regulator powers.
- **Adaptability expected in the Bill** that will enable it to evolve and add covered sectors over time.
- **Preparation timeline and recommendations** to comply with the Bill, including a detailed breakdown of strategic imperatives for organisations.

A New Standard for Supply Chains

Although the UK has inherited laws related to cyber security resilience from the European Union, the Bill comes as part of a recognition that it is time to bolster the UK's cyber regulations and move toward a distinctly national framework. The Cyber Security and Resilience Bill reflects the UK's intent to shape a risk-based approach which recognises supply chain risk not as a side concern but as a central vulnerability vector.

SecurityScorecard's data shows that over one in three breaches now stem from third-party vulnerabilities. This shift in attack patterns means supply chain security is now a compliance obligation, not just a discretionary investment. The Bill will set the tone for organisations to adopt continuous visibility and active risk governance across their digital supply chains.

Learning from NIS

While the UK charts its own path, lessons from existing directives, such as NIS2, may offer a glimpse into future enforcement expectations in the evolving regulatory framework in the UK. While UK policymakers move to build a distinct regulatory path, lessons from the EU's evolving directives and regulations, particularly the transition from NIS to NIS2, remain instructive.

NIS marked the EU's first region-wide, cohesive attempt to standardise cyber security responsibilities across critical and digital infrastructure providers. It crafted security responsibilities for those delivering essential services in five sectors and several digital services (operators of essential services (OES) and digital service providers (DSPs)):

- Transport
- Energy
- Drinking water
- Health
- Online marketplaces
- Search engines
- Cloud computing services

To address shifting risk, NIS2 widened its scope and applied more stringent expectations around incident reporting and supplier oversight. The UK's Cyber Security and Resilience Bill appears primed for a similar but distinct trajectory:

- NIS2 expanded the list of covered sectors to include 18 critical sectors, including:
  - More digital services, such as social platforms
  - Wastewater management
  - Product manufacturing
  - The space sector
- NIS2 introduced requirements for senior level responsibility in case of security lapses
- NIS2 introduced streamlined and stricter incident reporting requirements
- NIS2 mandates supply chain assessments, requiring organisations to evaluate and manage third-party security

Existing Cyber Security Regulations in the UK

Two comprehensive Post-Implementation Reviews conducted in 2020 and 2022 provide critical insight into the effectiveness of the NIS Regulations of 2018, which were derived from and share many of the same principles as the EU's NIS Directive. While these reviews found that the regulations have had a positive impact on organisational cyber posture, they identified systemic implementation challenges that necessitate legislative enhancement.

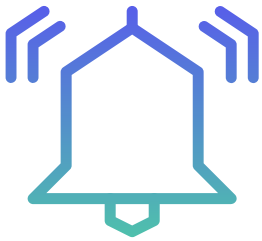
- **Implementation Velocity Concerns:** The reviews revealed that progress in regulatory compliance is "not fast enough," with just over half of affected operators updating their security policies since 2018.
    - This implementation lag reflects both the complexity of translating regulatory requirements into operational practice and insufficient regulatory mechanisms for ensuring timely compliance.
- **Scope Limitations and Coverage Gaps:** More significantly, the reviews identified critical coverage gaps in the current regulatory framework.
    - The existing focus on traditional critical infrastructure sectors failed to account for the increasingly interconnected nature of modern digital supply chains.
    - Managed service providers, data centres, and critical suppliers, which are often the actual vectors for successful attacks, remained outside direct regulatory oversight, creating systemic vulnerabilities that sophisticated threat actors routinely exploit.
- **Enforcement and Oversight Challenges:** The reviews also highlighted limitations in regulatory oversight mechanisms, particularly regarding supply chain risk management and incident reporting requirements.
    - Current frameworks lack sufficient granularity for assessing third-party security postures and fail to provide regulators with adequate visibility into cross-sector dependencies that amplify cyber risk.

Alarming Statistics Driving Legislative Action

The quantitative evidence supporting enhanced supply chain regulation is compelling and demonstrates the urgent need for systematic regulatory intervention:

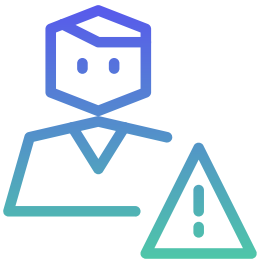
Supply Chain Attack Explosion: Supply chain attacks surged 431% between 2021 and 2023, with projections indicating continued growth through 2025, according to a report from Cowbell. This exponential increase reflects both threat actors' sophistication and the inherent vulnerabilities in current supply chain security practices.

Universal Third-Party Risk: Research indicates that 98% of organisations have experienced at least one breach involving a third-party vendor within the past two years. 97% of the top 100 UK organisations by market capitalisation had a third-party breach, according to SecurityScorecard's research. This near-universal exposure demonstrates that supply chain risk is not a theoretical concern but an operational reality that affects virtually every organisation.



Confidence Crisis: A UK government review found existing frameworks insufficient to protect national infrastructure, the economy, and essential services. Less than one-tenth of operators of essential services (OES) reported feeling confident in managing their supply chain risk. This lack of confidence reflects both the complexity of modern supply chains and the inadequacy of current risk management tools and frameworks.

Vulnerability Management Crisis: Europe sustains one of the slowest vulnerability remediation timelines compared to other regions, according to SecurityScorecard and Cyentia Institute research. European organisations are only remediating 25% of vulnerabilities within six months, and only reaching vulnerability remediation half-life in one year. This extended exposure window creates systematic vulnerabilities that threat actors can exploit across multiple supplier relationships.



For compliance professionals, these statistics highlight the inadequacy of current approaches and underscore the need for comprehensive, technology-enabled solutions that provide real-time visibility and control across complex supplier networks.

- The new Bill is expected to revolve around four core priorities:
- Expand the scope of regulated organisations
- Enhance regulatory oversight
- Streamline and clarify incident reporting
- Ensure regulation can adapt to evolving attacker behaviours

The Cyber Security and Resilience Bill will apply across the UK and progress through Parliament in 2025. While updates are still pending, the government has introduced the broad arcs of the plan in policy documentation, which provides key insights into who will need to update supply-chain risk management and just how they will need to adjust incident response plans and monitoring.

Designated Critical Suppliers

Crucially, the Bill would bring Managed Service Providers (MSPs) into scope. The Bill would enable regulators to recognise certain suppliers as "designated critical suppliers" (DCS) as well. This could help organisations bridge a gap in visibility and awareness, as the UK hasn't had a targeted way to address critical supply chain vulnerabilities under the 2018 regulations.

This is especially urgent in light of recent campaigns, including ransomware and state-linked espionage operations, that targeted supply chain vendors and MSPs to gain downstream access.

Detecting and responding to risk signals across entire ecosystems, including identifying vulnerable supply chain vendors, should now be an integral part of day-to-day compliance workflows, not left to annual assessments. The Bill is expected to introduce several key measures that will help drive this change:

- Regulators may designate a supplier as critical if its compromise could cause a "significant disruptive effect" on providing an essential service.
- For organisations that work with small digital service providers, or Relevant Digital Service Providers (RSDPs), the Bill may have a ripple effect in shoring up supply-chain risk. That's because small or micro RDSPs have been exempted from the 2018 regulations. This Bill will likely cover them.

It's All In The Data

The Bill may also bring data centres in scope, particularly those that are at or above 1MW capacity. (Enterprise data centres will fall in scope if at or above 10MW capacity.)

This update reflects the fact that data centres underpin critical digital infrastructure, from artificial intelligence (AI) workloads to public services, and are now targets for disruption. The Bill would make data centres responsible for implementing programs to manage cyber security risks and report significant incidents in line with other covered entities in the Bill.

Regulatory Strength

The Bill would strengthen regulatory authority, with provisions to tailor requirements by sector. Details are still emerging, but a likely component of regulators' enhanced authorities could enable them to apply sector-specific resilience requirements based on threat exposure and systemic impact.

The intent of this provision is to produce clearer expectations on what the government requires of organisations by sector, thereby raising security baselines across the board.

The Information Commissioner's Office (ICO) is also slated to expand its supervisory powers. In line with the policy expectations of the framework, the ICO would shift from reactive oversight to proactive cyber risk mitigation.

The UK government has hinted in policy documentation that regulators will also be able to establish a new cost recovery mechanism that can include invoices.

Incident Reporting Requirements

Like the transition from NIS to NIS2, the new regulation would raise expectations for incident reporting and transparency. The Bill is expected to expand incident reporting criteria, update incident reporting timelines, and require more transparency from digital services and data centres.

- Organisations in the UK must prepare to report an incident within 24 hours of becoming aware of an incident in line with the proposed Bill. They must then provide an incident report within 72 hours.
- The Bill may also address a perceived narrow implementation of the current NIS regulations, with reporting requirements for incidents that interrupt the continuity of an essential or digital service. This leaves out key incidents that pose major risks to critical infrastructure in the UK.
- Notably, the Bill could require organisations to report incidents that carry the potential to significantly affect essential services.
- The Bill could also prompt organisations to report on incidents that affect the confidentiality, integrity, and availability of a system. This can include compromises related to data confidentiality, spyware attacks, and attacks that leverage break-ins at MSPs and other firms in order to compromise multiple organisations.
- When firms providing digital services and data centres are the target of a breach, the new Bill would require alerts to customers who might be affected as well.

> **"Transparency requirements will raise standards across service providers, and customers will be better informed when the service they rely on could be affected or have a knock-on effect on their business."**
>
> — Cyber Security and Resilience Bill Policy Statement

Incident response under the new Bill reflects a more aggressive posture. For organisations managing hundreds or thousands of vendors, this raises critical operational questions: Who is watching your suppliers? How quickly can you triage risk?

Implementing continuous monitoring to detect and respond to vulnerabilities and indicators of compromise (IOCs) will give organisations the speed and context required to meet incident reporting thresholds and coordinate response at scale.

These changes also represent a call for organisations to map their security posture and vendors' security postures against regulatory benchmarks if they are not already doing so.

UK Cyber Security and Resilience Bill v. NIS2

The UK Cyber Security and Resilience Bill would place supply chain resilience at the forefront of regulatory priorities, in many respects mirroring recent updates under the NIS2 Directive. While the precise text is still evolving, organisations may anticipate closer alignment with EU expectations in the months ahead.

Importantly, the Bill would expand the legal definition of in-scope organisations—particularly data centres and managed service providers, paving the way for baseline cyber security postures to match the risk profile of 2025.

The scope of the developing framework echoes the NIS2 updates, which expanded sectors with applicable responsibilities. The Bill is also likely to expand the scope of which businesses and sectors must comply.

The Bill is expected to provide flexibility for the government to add more sectors that must comply without requiring an Act of Parliament. This change may signal this Bill is just the beginning of cyber regulation updates in the UK.

The Bill will likely allow regulators to take a more proactive role in monitoring security compliance, including the ability to recover costs.

The Bill would strengthen incident reporting obligations. Regulated organisations would be required to report "significant cyber incidents" within a day of discovery, bringing UK timelines in line with the 24-hour breach notification standard under NIS2. This further promotes alignment between UK and EU expectations.

The Bill would also mandate broader and faster reporting of incidents in part to provide the government better visibility into threats.

Side-By-Side Comparison

	CYBER SECURITY AND RESILIENCE BILL	NIS2
Region	**UK**	**EU**
Scope	• Slated to include Managed Service Providers (MSPs) to increase oversight of digital services. • May expand to data centres and other sectors without further legislation.	**Covers 18 sectors:** 1. Energy 2. Transport 3. Banking 4. Financial market infrastructures 5. Health 6. Drinking water 7. Waste water 8. Digital infrastructure 9. ICT service management 10. Public administration 11. Space 12. Postal and courier services 13. Waste management 14. Manufacture, production, and distribution of chemicals 15. Production, processing, and distribution of food 16. Manufacturing 17. Digital providers 18. Research
Third-Party Focus	• Focuses on "designated critical suppliers" (DCS). • Stronger focus on MSPs.	• Emphasises supply chain security across essential and important entities.
Reporting Standards	• Report incidents within 24 hours. • Full report within 72 hours.	• Report incidents within 24 hours. • Additional report within 72 hours. • Additional report within 1 month.
Enforcement	• Expected to grant regulators proactive powers such as cost recovery.	• Harmonised enforcement across member states.

The Bill reflects the UK's intent to improve visibility into cyber threats and supply chain risk, much like NIS2, so that it can enable stronger defence and update regulatory frameworks to keep pace with current attack trends. As the thinking goes, the Bill may catalyse a feedback loop of improved cyber posture, driven by regulatory oversight and sector resilience.

As organisations prepare for implementation of the Bill, aligning internal processes with both NIS2 and the Bill will be essential to staying compliant and resilient.

Evolving To Match Adversary Tactics

The Bill is coming at a time when threat actors are no longer coming through the front door, causing disruption throughout the UK. The Bill is slated to confront the reality of these indirect attacks, supply chain compromise, and the national consequences of third-party digital exposure.

The United Kingdom faces an unprecedented cyber threat environment that has fundamentally shifted the risk calculus for organisations across all sectors. The National Cyber Security Centre (NCSC) characterizes the current threat landscape as "diffuse and dangerous," reflecting both the proliferation of threat actors and the increasing sophistication of attack methodologies that existing regulatory frameworks struggle to address effectively.

In the King's Speech in July of 2024, the government announced that it would be introducing the new Bill as part of an acknowledgement that the UK's legal and regulatory frameworks have not kept pace with threat actor behaviour at great cost.

Quantified Economic and Operational Impact

The financial implications of cyber threats have escalated dramatically in recent years in the UK. Current estimates place the annual cost of cyber threats to the UK economy somewhere between £27 billion to £30.5 billion, according to the UK government and research from Beaming, respectively. This represents a substantial increase from earlier assessments and highlighting the accelerating economic burden of inadequate cyber resilience.

The UK Government's Cyber Security Breaches Survey 2024 reveals that UK businesses experienced approximately 7.78 million cyber crimes in the past year alone, demonstrating the scale and frequency of successful attacks against UK organisations—and the need to change course.

Attackers on the Hunt

Malicious actors are always adapting their attack tactics, techniques, and procedures (TTPs) to evade detection and exploit systemic weaknesses. And as digital supply chains expand and systemic risks increase, outdated policies and inconsistent security standards have created serious vulnerabilities across both public and private sectors.

Recent breaches reflect the urgency of the moment:

- A wave of high-impact cyber incidents in recent months has intensified the need to bolster cyber resilience throughout the UK.
- The attacks on the Ministry of Defence and UK healthcare entities, for instance, showed just how these attacks can spillover into the physical world and cause real harm: In 2024, a healthcare hacking campaign delayed care for over 10,000 patients, according to the UK government—and may have contributed to at least one reported fatality.
- The Cloud Hopper campaign, linked to China-based actors, targeted managed service providers (MSPs) around the globe, offering lessons in third-party resilience. The operation allowed hackers to exfiltrate data from MSPs and major customers, underlining the persistent nature of the current threats that organisations face.

These campaigns underline what defenders have long known—that as organisations continue to rely on third parties and service providers, attackers increasingly rely on indirect access. They're compromising third parties, software vendors, and cloud platforms to break in and pivot, causing further damage to countless other entities.

Enterprising threat actors are typically looking to maximise their economic impact and work as little as possible, and using just a handful of flaws to break into hundreds or thousands of organisations instead of creating new attack playbooks each time just makes economic sense.

SecurityScorecard's breach research confirms the trend. Third-party suppliers are a growing vector of compromise. And without persistent monitoring and validated risk data, organisations risk being blindsided by exposures several layers removed from their own perimeter.

- In one 2024 campaign, the ransomware group C10p breached organisations in a sweeping campaign using just a few vulnerabilities in Cleo file transfer software.
- In the MOVEIt campaign, C10p breached hundreds if not thousands of organisations in a series of cascading breaches.
- State-linked actors with ties to China are particularly active as well. After ransomware threat actors, China-linked groups were the most active actors targeting third-party suppliers globally over the past year, according to SecurityScorecard research.

Even well-defended organisations remain vulnerable if their third- and fourth-party suppliers are unmonitored and unassessed. Visibility into your dependencies and being able to take action before it's too late is essential in 2025.

State-Sponsored and Organized Crime

The NCSC Annual Review 2024 highlights another concerning evolution in the capabilities of threat actors, with persistent attacks from hostile states increasingly coordinating with organized criminal enterprises as well. This convergence has created a threat ecosystem where nation-state resources and criminal innovation combine to target UK critical infrastructure with unprecedented effectiveness.

For compliance professionals, this represents a fundamental shift from traditional risk models that treated state and criminal threats as distinct categories requiring separate mitigation strategies.

Mind the Gap

The Bill is a targeted response to shortcomings in UK cyber policies that have lagged behind threat actors' learning curve. The Bill appears to directly target these structural gaps. The Bill's objectives are clear: Strengthen national cyber defences, secure vital infrastructure, and ensure that the digital services supporting government and business are resilient in line with the threats they face.

This approach recognises that cyberattacks cause cascading, real-world disruptions, from disrupted patient care to persistent data exposure. For compliance professionals, updating cyber security risk management programs and compliance programs to align with the proposed regulatory framework as it develops will help organisations stay one step ahead of hackers.

Of particular interest, the upcoming Bill seeks to address the escalating threat of ransomware by mandating increased incident reporting to give the government better data on cyber attacks. With 41.4% of ransomware attacks now stemming from the supply chain, controlling supply-chain risks in accordance with the Bill is more urgent than ever.

UK organisations are also tracking the complementary ransomware payments ban and reporting proposals under consultation by the UK Home Office. While distinct from the UK Cyber Security and Resilience Bill, the UK government has signaled that both efforts will align without duplicating efforts.

Threat Landscape Takeaways

- Adversaries have shifted from isolated attacks to scalable campaigns that target systemic weaknesses, such as shared technology platforms or weakly governed supplier ecosystems. Without continuous monitoring and coordinated threat sharing, these tactics bypass perimeter defences and exploit trust-based access.
- Attackers with nation-state backing are increasingly coordinating with organised criminal enterprises, calling for a shift in mitigation and compliance strategies.
- This evolution in TTPs has elevated the UK's essential services as high-value targets, particularly when they intersect with politically sensitive functions like healthcare, national security, and local governance.

These incidents and attack patterns illustrate a clear trend: Threat actors are shifting focus toward high-impact, high-leverage targets. Organisations in the UK must not only catch up to these changes—they must anticipate them.

Investments in continuous monitoring, Third-Party Risk Management (TPRM), and threat intelligence are essential to bridge the gap between adversary tactics and national resilience.

Building a Bill to Adapt to a Changing World

Organisations should be prepared to continuously monitor their alignment with the Bill's framework, because just as attackers evolve, it is expected to grow and evolve in response to changed attacker behaviour. The foundational understanding that threat actors are constantly evolving their methods is built into the policy itself.

New Powers in the Bill

The policy statement on the Bill notes that the Secretary of State would gain powers to update the regulatory framework without an Act of Parliament, for instance.

This can also enable the Bill to stay up-to-date with technological advancements and specific risks as they emerge.

For UK organisations keeping pace, this means constantly staying abreast of vulnerabilities as they emerge in near real-time, continuously monitoring cyber practices of third and fourth parties, and moving beyond point-in-time audits. Security and compliance checkups in the context of the Cyber Security and Resilience Bill must be iterative and must be continuous.

Sector Updates

Even sectors that don't fall in scope at present must pay attention. The Secretary of State may add new sectors or subsectors as technology or vulnerabilities dictate, according to the policy documentation on the Bill. Organisations that are able to evade scrutiny today may face a different threat environment tomorrow and need to quickly adapt.

Zooming out, the takeaway is clear: Gaining control of supply chain risk has never been more important in the UK. Together, these regulatory changes will mark a systemic shift in how the UK expects organisations to manage risk, build cyber resilience, and stay abreast of threats.

> **"New technologies and emerging threats require agile regulations. It is important for national security that our regulatory framework is not stagnant."**
>
> — Cyber Security and Resilience Bill Policy Statement

Meeting the Speed of Risk

Legacy assessments and static audits no longer meet legal or operational expectations in 2025. They also fail to reflect the pace and scale of today's exploitation patterns. Security threats now move faster than compliance cycles, and the organisations best positioned to respond aren't just meeting regulatory expectations. They're operating with real-time visibility into supply chain risks and threat actor behaviour.

Continuous Monitoring for Compliance Success

Organizations that become Designated Critical Suppliers (DCS) under the UK's new legislation will need comprehensive capabilities to meet enhanced regulatory requirements. SecurityScorecard offers the full breadth of solutions to help organizations meet the Bill's third-party and supply chain requirements across multiple levels of engagement:

- **Self-Service Platform Access:** Direct access to SecurityScorecard's rating and monitoring capabilities for organisations developing internal TPRM programs
- **Professional Services Support:** Expert guidance for implementing comprehensive supply chain risk management programs aligned with UK regulatory requirements
- **Managed Service Solutions:** Full-service TPRM program management through MAX for organisations requiring comprehensive external support

Organisations seeking to prepare for compliance in line with the Bill's core requirements will need comprehensive capabilities that enable compliance success while improving overall business resilience. Organisations can address these challenges with continuous visibility into third-party risk posture through SecurityScorecard by:

- **Mapping cyber risk signals** key to compliance controls
- **Monitoring vendor exposures** and automating discovery
- **Preparing documentation for audits** or attestations

Teams that unify continuous monitoring with threat intelligence will be able to proactively defend and prepare for compliance, since authorities are crafting the Bill so that it evolves in sync with threats in the future. Intelligence feeds from SecurityScorecard can pipe directly into SIEM, SOAR, or TIP tools, providing real-time data that helps security teams keep active threats out.

Preparation Timeline and Recommendations

The successful implementation of the Cyber Security and Resilience Bill requirements demands systematic preparation and strategic investment in enhanced cyber security capabilities. Organisations that begin preparation now will position themselves to achieve compliance efficiently while gaining competitive advantages through improved resilience and operational security.

Why immediate action in 2025 is imperative

Organisations must begin comprehensive preparation activities immediately to ensure readiness for implementation in 2026.

Conduct Supply Chain Risk Assessments Aligned with the NCSC Framework

Organisations must immediately conduct comprehensive supply chain risk assessments aligned with the NCSC Cyber Assessment Framework (CAF). These assessments should:

- Identify critical suppliers
- Evaluate their security postures
- Determine potential designation as Designated Critical Suppliers (DCS)

The assessment process should include a comprehensive inventory of all supplier relationships, as well as an effort to map dependencies on essential services, evaluate supplier security controls against regulatory requirements, and identify potential single points of failure within the supply chain. This baseline assessment provides the foundation for all subsequent compliance activities, enabling organisations to prioritize their preparation efforts effectively.

Review Current TPRM Capabilities Against Bill Requirements

Organisations must conduct thorough gap analyses of their current third-party risk management capabilities against the anticipated requirements of the Bill. This evaluation should assess existing monitoring systems, reporting capabilities, incident response procedures, and regulatory compliance frameworks.

The gap analysis should also:

- Identify specific technology investments required to achieve compliance
- Assess current staffing and expertise needs
- Evaluate existing supplier contracts for security requirements
- Determine the need for external support services

Organisations that identify significant gaps should initiate procurement processes immediately to ensure adequate preparation time.

Begin Stakeholder Engagement with Critical Suppliers

Immediate engagement with critical suppliers is essential to ensure their readiness for potential DCS designation and enhanced security requirements. This engagement should include notification of upcoming regulatory changes, assessment of supplier willingness and capability to meet enhanced requirements, and collaborative development of implementation timelines.

- Organisations should also begin updating supplier contracts to:
- Include enhanced security requirements
- Establish regular security assessment schedules
- Develop collaborative incident response procedures

Early supplier engagement offers the best opportunity to address potential compliance issues before they escalate into regulatory violations.

Medium-term Implementation (2025-2026)

Implement Enhanced Monitoring and Reporting Systems

Organisations must implement comprehensive monitoring and reporting systems capable of meeting the Bill's enhanced requirements for incident reporting and ongoing compliance demonstration. These systems should provide continuous visibility into supplier security postures, automated compliance reporting capabilities, and integration with existing security operations.

The implementation should include:

- Continuous monitoring platforms
- Integration with threat intelligence feeds
- Automated alerting and escalation procedures
- Comprehensive documentation systems for regulatory reporting purposes

Organisations should prioritize solutions that can scale with their supply chain complexity and adapt to evolving regulatory requirements.

Establish Designated Critical Supplier (DCS) Identification and Management Processes

Organisations must develop systematic processes for identifying, managing, and monitoring DCS. These processes should align with regulatory guidance and provide comprehensive oversight of DCS relationships.

The management processes should include formal DCS designation procedures, enhanced security requirement

implementation, regular performance monitoring and assessment, and escalation procedures for non-compliance issues.

Organisations should also establish collaborative relationships with regulators to ensure the appropriate designation of DCS and ongoing compliance monitoring.

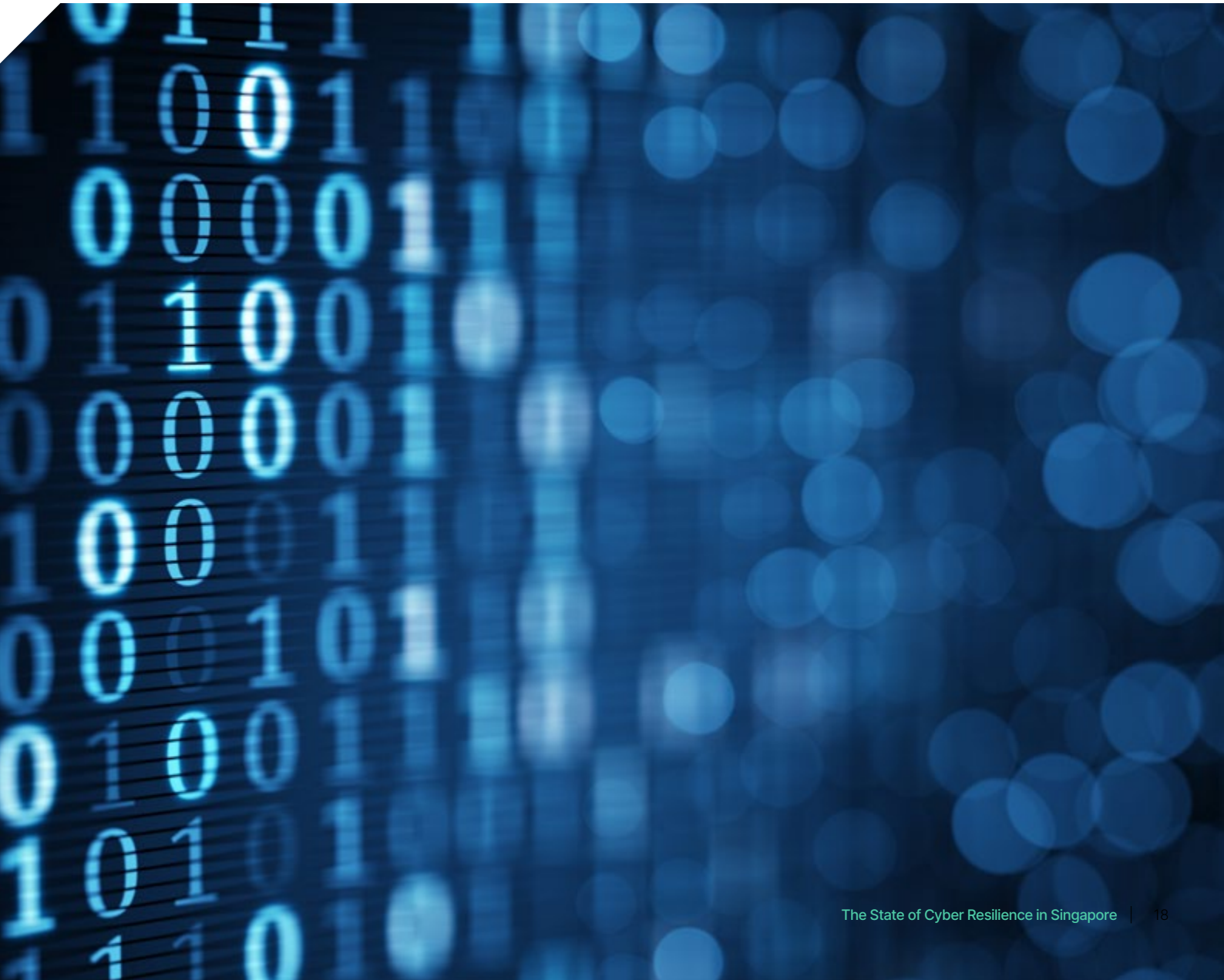
Update Incident Response Procedures for Mandatory Reporting

Organisations must update their incident response procedures to meet the proposed framework's reporting requirements. These procedures should ensure the rapid identification, assessment, and reporting of relevant incidents within the required regulatory timeframes of 24 hours and 72 hours.

The updated procedures should include:

- Specific escalation criteria for different incident types
- Standardized reporting templates and processes
- Integration with regulatory reporting systems
- Coordination procedures for engagement with law enforcement and regulatory authorities

Organisations should also conduct regular exercises to ensure the effectiveness of their procedures and staff readiness.



Strategic Imperatives for Organisations

Comprehensive Supply Chain Oversight

Organisations must implement mandatory evaluation and ongoing monitoring of critical suppliers, moving beyond traditional contractual approaches to technology-enabled continuous risk assessment. This requires investment in TPRM platforms that provide real-time visibility into supplier security postures and automated compliance reporting capabilities.

Enhanced Incident Response

The proposal's emphasis on enhanced reporting capabilities for supply chain security incidents necessitates the systematic improvement of incident response procedures and their integration with regulatory reporting systems. Organisations must develop the capacity for rapid incident identification, assessment, and reporting within the specified regulatory timeframes of 24 hours and 72 hours.

Proactive Risk Management

The legislation demands a fundamental shift from compliance-driven to resilience-focused approaches, emphasizing continuous improvement and adaptation to emerging threats. This requires investment in threat intelligence, continuous monitoring systems, and adaptive security frameworks that can evolve in response to the changing threat landscape, just as the Bill will.

Final Thoughts: Resilience Requires Ecosystem Accountability

A Resilient Future

The UK's Cyber Security and Resilience Bill, along with the EU's NIS2 Directive, firmly signal the shift from perimeter-based security to supply chain-wide accountability. Organisations must now protect their extended enterprise, from internal infrastructure to the far edges of the supply chain.

As the UK works to overhaul its cyber regulatory framework, compliance will demand continuous monitoring, cross-functional governance, clear visibility, and accountability—especially as the scope of covered organisations expands and as incident reporting requirements emerge.

Organisations that proactively prepare will not only meet the new requirements but build long-term operational resilience and trust. Those that delay could risk regulatory scrutiny, reputational damage, and avoidable breaches.

SecurityScorecard's Supply Chain Detection and Response (SCDR) solution equips organisations with the intelligence, visibility, and automation needed to meet regulatory obligations and safeguard supply chains. Whether your organisation is a DCS or whether your organisation needs to take control of its supply chain, SecurityScorecard's MAX managed services and platform provide the tools to monitor supply-chain risk, align with compliance needs, and respond quickly to emerging threats.

>>> EXPLORE SCDR >>> EXPLORE MAX

To learn more and create your free account, visit SecurityScorecard.com

ABOUT SECURITYSCORECARD

SecurityScorecard created Supply Chain Detection and Response (SCDR), transforming how organizations defend against the fastest-growing threat vector—supply chain attacks. Our industry-leading security ratings serve as the foundation and core strength, while SCDR continuously monitors third-party risks using our factor-based ratings, automated assessments and proprietary threat intelligence, to resolve threats before they become breaches. MAX enables response and remediation capability, working through our service partners to protect the entire supply chain ecosystem while strengthening operational resilience, enhancing third-party risk management, and mitigating concentrated risk.

Trusted by over 3,000 organizations—including two-thirds of the Fortune 100—and recognized as a trusted resource by the U.S. Cybersecurity & Infrastructure Security Agency (CISA). Backed by Evolution Equity Partners, Silver Lake Partners, Sequoia Capital, GV, NGP, Intel Capital and Riverwood Capital, SecurityScorecard delivers end-to-end supply chain cybersecurity that safeguards business continuity. For more information, visit securityscorecard.com or connect with us on LinkedIn.

SecurityScorecard

SecurityScorecard.com
info@securityscorecard.io