Risk Ledger

Every Link Matters: The State of Supply Chain Security 2026 — UK Edition

A Risk Ledger Data Insights Report

About Risk Ledger

Risk Ledger is a network-first platform delivering Active Supply Chain Security. We move beyond architecturally flawed TPRM to deliver continuous, collaborative defence for security and risk teams, because every link matters.

Founded in 2018, Risk Ledger pioneered the network-first approach to supply chain security. At the core of our platform is a standardised TPRM Engine that replaces repetitive questionnaires with a single, continuously updated supplier profile shared across the network. This builds a vast interconnected database of supplier security data and provides organisations with instant access to standardised, trusted assessments across a growing network.

Unlike spreadsheets and point solutions that trap you in endless manual reviews, Risk Ledger visualises your supply chain as it really exists, revealing nth-party vulnerabilities, hidden concentration risks and changing supplier relationships, so you can detect and respond to emerging threats before they cascade through your ecosystem.

Our platform already connects 16,000+ organisations across the UK's most critical sectors - from financial services to the public sector - enabling them to share intelligence, identify systemic vulnerabilities, and coordinate responses that no single organisation could achieve alone.

By leveraging network-level insights, ecosystem mapping and emerging threat detection with Risk Ledger, you optimise the entire ecosystem's resources and Defend-as-One.

Risk Ledger Ltd.
Adam House
7-10 Adam Street
London WC2N 6AA
United Kingdom

Company registration number (England & Wales): 10831970

Contact: www.riskledger.com | marketing@riskledger.com

Foreword

In 2026, supply chain cyber security remains a persistent challenge. Incident rates are high and threat actors are increasingly sophisticated, yet risk management remains stuck in an outdated cycle of isolated, bilateral assessments. The findings of our new survey demonstrate that significant operational gaps remain: most organisations still require weeks to onboard a supplier and are unable to map breach exposure within 24 hours. These structural shortcomings occur in a worsening environment shaped by state-sponsored sabotage and the concentration risks introduced by the rapid adoption of AI across the supply chain.

Over the past few years, Risk Ledger has consistently argued that traditional third-party risk management is no longer enough. We have actively pioneered a network-first approach to provide deep-tier visibility and unmask concentration risks at firm and sectoral level at a time when there was still little appreciation in the wider market of how these shared dependencies cluster. We are pleased to see that this realisation is now widely shared on the global stage, as evidenced by the World Economic Forum dedicating a critical part of its latest *Global Cybersecurity Outlook 2026* to the systemic threats of supply chain interdependencies and concentration risk. What has long been championed as an advanced defensive model by Risk Ledger is now increasingly recognised as the definitive framework required for modern operational resilience.

Digital supply chains are shared infrastructure. Resolving our current vulnerabilities requires a structural evolution rather than simply executing more traditional TPRM. We must implement standardised assessment frameworks to eliminate duplicated effort, transition from periodic to continuous monitoring, and map the shared dependencies that create systemic vulnerability. The true solution lies in collaborative visibility, evolving TPRM from a siloed risk management exercise into an active cyber defence discipline through Active Supply Chain Security (ASCS). We can only secure these complex networks by looking at them together.

Together, we can Defend-as-One.

Haydn Brooks,
CEO & Co-Founder, Risk Ledger

Contents

The State of Supply Chain Security in 2026

Supply chain cyber security has become a central resilience issue for UK organisations, the wider economy and national security. Incidents in recent years have shown how quickly a disruption at widely used suppliers can affect multiple organisations at once. This is a key reason why supply chain cyber security has moved from being treated as a procurement or compliance issue to a broader resilience and national security concern, and also leading regulators to place growing emphasis on the dependency chains that are sitting beneath important business services.

Risk Ledger's 2025 report, Every Link Matters: The State of Supply Chain Security 2025 – UK Edition, sets the baseline for this year's analysis. It showed that supply chain cyber incidents had become common across UK organisations; that traditional third-party risk management (TPRM) was proving too slow, too static and too narrowly focused to keep pace with the extent of the threat; and that limited visibility beyond direct suppliers was preventing organisations from identifying deeper dependencies and hidden concentration risks. Those findings remain the starting point for this year's report.

The 2026 edition, however, pivots in two major ways. Rather than just revisiting whether supply chain risk is significant, or whether existing practices have shortcomings, it examines how far organisations have already moved towards a more operational model of supply chain security: one in which supplier data is more standardised and reusable, critical suppliers are monitored on a continuous basis, exposure can be mapped quickly when incidents occur, and collaboration with peers helps identify risks that no single organisation can see alone. It also extends the lens from organisational resilience to sectoral resilience, reflecting the reality that many UK organisations depend on the same platforms, service providers and subcontractors, and that regulators are increasingly focused on the resilience of important services at sector level.

The sections that follow explore this transition from four angles: the evolving threat and regulatory environment; the current state of TPRM outcomes; the emerging model of Active Supply Chain Security; and how sector-level collaboration in Risk Ledger communities is advancing this model in practice.

Why this report now

- Supply chain incidents remain common and high impact for UK organisations.
- New UK/EU rules demand deeper visibility and stronger resilience.
- Fresh 2026 survey data shows traditional TPRM is still too slow and siloed.
- The report sets out Active Supply Chain Security as a new model.

Section 1: Supply Chain Cyber Security Threats and Regulations in 2026

1.1. Supply Chain Cyber Security Threats Facing UK Organisations

The extent of the cyber threat facing UK organisations has not eased since the previous edition of this report. In April 2026, Dr Richard Horne, CEO of the National Cyber Security Centre, told the CYBERUK conference in Glasgow that the UK is confronted with a "perfect storm": the convergence of rapid technological change driven by AI and sustained geopolitical tension is creating a period of "tumultuous uncertainty". In his assessment, "the majority of the nationally significant incidents that my team is handling now originate directly or indirectly from nation states."

Supply chains meanwhile remain a primary attack vector through which threat actors target organisations. However, the UK government's Cyber Security Breaches Survey 2025/2026, published in April 2026, found that just 15% of businesses formally review the cyber risks posed by their immediate suppliers, and only 6% review their wider supply chains. These figures have remained largely unchanged from the previous year, despite the proliferation of high-profile supply chain incidents.

The WEF Global Cybersecurity Outlook 2026 found that 65% of large organisations now cite third-party and supply chain risks as their primary cyber resilience challenge — up from 54% the year before. Nonetheless, supply chain risk management is still being treated by most organisations as a compliance exercise rather than a dynamic, continuous risk management process; just 27% simulate cyber incidents with supply chain partners, and only a third comprehensively map their supply chain ecosystems.

What changed since 2025

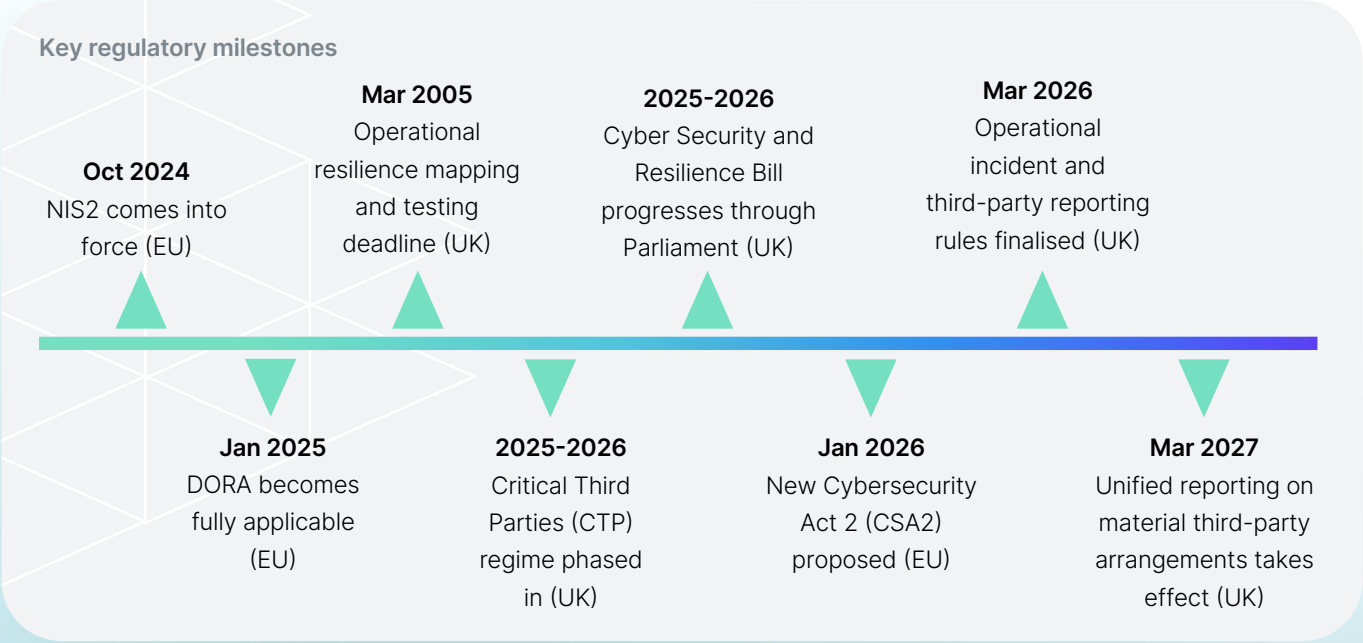
- State-sponsored attacks has become the new normal in major supply chain incidents.
- Attackers are increasingly using AI to find and exploit vulnerabilities at scale.
- Regulators are shifting from firm-by-firm oversight to sector-wide mapping of dependencies.
- Supply chain security is now treated as a resilience and national security issue, not just a firm-level compliance function.

The rapid adoption of AI, meanwhile, has created a whole new category of cyber risk in organisations' supply chains. Frontier AI models are "rapidly enabling discovery and exploitation of existing vulnerabilities at scale", according to Dr Horne. For organisations, however, the risk is not only that adversaries will use AI to attack them directly with more ease and speed, and perhaps even precision. It is that suppliers are themselves adopting AI-based services at scale — often built on a small number of foundational models — introducing new vulnerabilities and new concentration risks into the extended supply chain that customer organisations have limited visibility of and almost no contractual control over.

1.2. DORA, NIS2 and UK Supply Chain Security Regulations

UK and EU regulators have responded to this changing threat landscape with new rules and guidelines that, taken together, represent a fundamental shift in what is expected of regulated entities and their critical suppliers. The common thread running across these new regulatory regimes is the move from firm-level compliance towards an increased emphasis on evidence-based, continuously managed understanding of risk across the extended supply chain supporting critical services as well as on sectoral resilience.

In the EU, the Digital Operational Resilience Act (DORA) came into full application in January 2025. It requires financial entities to manage ICT concentration risk explicitly — not just at the level of direct third-party providers, but across subcontractors and deeper-tier dependencies that contribute to critical or important functions. Article 29 of DORA requires firms to assess whether envisaged ICT arrangements would create substitutability risk or excessive dependence on a single provider, and to consider the downstream consequences where subcontracting is taking place. The European Supervisory Authorities are also developing an oversight framework for Critical ICT Third-Party Providers, giving regulators direct supervisory powers over the most systemically important technology suppliers to the financial sector.



The European Commission's newly proposed Cybersecurity Act 2 (CSA2) meanwhile — introduced in January 2026 — places a heavy dual emphasis on regulatory standardisation and supply chain visibility. To tackle market fragmentation, the proposal overhauls the European Cybersecurity Certification Framework (ECCF), creating streamlined, EU-wide standards that allow firms to certify their broader "cybersecurity posture" to easily prove compliance across the entire single market. The Act is also expected to require organisations to map out their digital dependencies deeply enough to uncover and phase out components from designated "high-risk suppliers" or jurisdictions posing non-technical, geopolitical risks.

In the UK, the operational resilience rules introduced by the Bank of England, FCA and PRA (PS21/3 and the associated supervisory statements) came into full effect in March 2025. They require firms to identify their most important business services, set impact tolerances, and demonstrate that they can remain within those tolerances during severe disruption — including disruption originating in their supply chains.

To map these dependencies across the sector, the newly finalised operational incident and third-party reporting rules (FCA PS26/2 and PRA PS7/26, published in March 2026) will require firms to submit standardised registers of all material third-party arrangements by March 2027. This data-driven mechanism effectively creates the evidence base for the critical third parties regime (PS16/24 and PS24/16), which extends regulatory reach directly to the most systemically important providers to the UK financial sector, enabling the PRA and FCA to set resilience requirements for suppliers whose disruption could threaten financial stability.

The Cyber Security and Resilience Bill, introduced to Parliament in November 2025, represents the most significant update to the UK's cross-sector cyber legislation since the 2018 NIS Regulations. It also introduces a new Designated Critical Suppliers regime that allows regulators to place direct statutory cyber security duties on suppliers whose disruption could cause widespread harm to

essential or digital services. The government's own framing of the Bill uses the Synnovis/NHS attack as the defining illustration of what this regime is designed to prevent: a single supplier breach causing cascading disruption across multiple critical services.

These frameworks also share a common logic that goes beyond requiring firms to manage their own supplier relationships better. Across both the UK and the EU, regulators are systematically collecting structured data on the suppliers that support critical and important business functions — including subcontractors and deeper-tier dependencies — with the explicit aim of arriving at a more complete sector-level picture of who depends on whom.

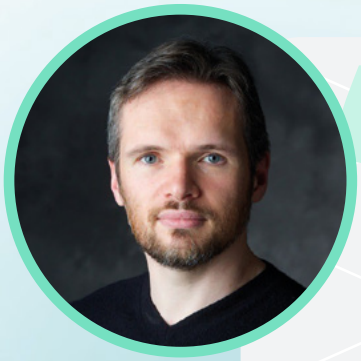
This is the point that most TPRM programmes have not yet fully appreciated. Regulators are not simply asking regulated entities to demonstrate due diligence. They are using the data those entities provide — on their suppliers, their subcontractors, their technology dependencies — to assemble a map of the wider sectoral supply chain. That map is what would allow supervisors to identify potential single points of failure, assess concentration risks at sector scale, and make informed decisions about which suppliers warrant direct regulatory designation and oversight.

The 2026 survey findings, examined in the next section, provide a measure of how far UK organisations have progressed towards those capabilities.

1.3. Changing Expectations

Taken together, the threat and regulatory pictures point to the same conclusion. Supply chain cyber risk is becoming more dynamic, more interconnected and more consequential, while regulatory expectations are increasingly focused on visibility into deeper dependencies, resilience of important services, and the identification of systemic risk.

This has an important implication for the rest of the report. The question is no longer simply whether organisations recognise supply chain cyber risk as serious. It is whether the tools and practices they still rely on are capable of meeting the speed, visibility and operational demands of this new environment. The next section addresses that question directly by examining the 2026 survey findings on current TPRM outcomes, including incident prevalence, onboarding speeds, visibility gaps and incident response readiness.



> “Identifying systemic risks is really important. However in most cases, only industry-level associations have enough combined resources and adequate information sharing guardrails in place to efficiently identify actual systemic risks, agree actions and, with the help of regulators, influence large players in the supply chain.”

Yohann Le Grand, Senior Security & Resilience GRC Manager, Lloyds Wealth

Section 2: Third-Party Risk Management (TPRM) Trends in 2026

86%

of respondents identified supply chain incidents among their top three areas of concern.

2.1 Section Overview

The previous section set out the changing threat landscape facing organisations in the UK and why regulators are placing growing demands on the effective management of supply chain cyber risk across entire sectors. This section examines how well organisations are doing in responding to these new realities and pressures in practice. Drawing on a survey of 500 UK cyber security and third-party risk management professionals conducted for this report, we measure current performance across four dimensions: incident prevalence and threat perception; onboarding and assessment review speeds; supply chain visibility; and incident response readiness.

2.2 Measuring Current Outcomes

The 2026 survey suggests that the core picture that emerged from last year's report has not fundamentally changed. Supply chain incidents remain widespread: 82.4% of respondents said they had experienced at least one incident in their supply chain in the previous 12 months, with 41.8% reporting two incidents and 5.4% reporting three or more. This compares to 85% of organisations with at least one incident in the 2025 report, indicating that incidents remain stubbornly persistent. The level of concern about supply chain incidents expressed by the surveyed industry professionals tracks closely with this experience. 86% of respondents still identified such incidents among their top three areas of concern for 2026, only somewhat down from 90% in 2025.

82.4%

of respondents experienced at least one supply chain incident in the last 12 months, with 47.2% experiencing two or more.

2.3 Supplier Security Due Diligence Remains Slow

One of the clearest indicators of the limitations of today's TPRM model is the speed, or lack thereof, with which organisations can complete due diligence on new suppliers. In the 2026 survey, only 38% of respondents said their organisation can complete security due diligence when onboarding a new supplier within two weeks, while 34.6% of organisations require three or more weeks, and 12% require more than one month to do so.

34.6%

of respondents take 3 weeks or more to complete security due diligence for new suppliers.

These figures matter because the lack of onboarding speed is not just a procurement bottleneck. When risk assessment processes take weeks or months, organisations are forced into difficult trade-offs between commercial urgency and security assurance. Slow due diligence can delay the adoption of critical suppliers, create friction with business teams, and encourage workarounds that weaken oversight. It also signals that many current TPRM processes remain heavily manual, heavily bespoke, and difficult to scale consistently across a large supplier estate.

The results reinforce a broader structural problem: traditional TPRM tends to be bilateral, organisation-to-individual supplier, questionnaire-led, and labour-intensive. That makes it hard to move quickly, particularly when teams are dealing with hundreds or thousands of suppliers and where each review requires separate documentation, follow-up and interpretation. The consequence is that many organisations can only apply the most intensive assurance to a relatively small subset of suppliers, leaving the wider supply chain subject to lighter-touch or infrequent scrutiny.

2.4 The Supply Chain Visibility Gap

Limited supply chain visibility remains another defining weakness of the current model. In the 2026 survey, 30% of respondents said they have full visibility into the entire chain of subcontractors contributing to their important business functions. A further 50.2% said they have high visibility into all direct subcontractors of their critical third parties, while 16% reported only partial visibility into some fourth parties of their critical suppliers. Only 3% of respondents to our 2026 survey said they have no visibility beyond direct critical third parties at all, a marked improvement from last year.

This is one of the most important findings in the report because it highlights how far the average organisation has come in terms of gaining better visibility into their supply chain dependencies beyond their direct critical suppliers, at least into critical fourth parties, but it also reveals how far we still have to go in gaining a much better understanding of our real exposure to the full depth of today's intricate digital supply chains. In practice, this means many organisations still cannot easily trace which deeper-tier dependencies support their critical business services, where common failure points may exist, or how disruption might spread through the extended chain of supply chain dependencies during a cyber incident.

This persistent visibility gap is also increasingly misaligned with the direction of regulation. As we noted in the previous section, UK and EU resilience rules are moving toward deeper mapping of important business services, critical dependencies and subcontracting chains. The survey findings suggest that many organisations still have some distance to go before being able to meet these expectations in a more complete way.

56%

of respondents can't map their extended supply chain's exposure to an emerging threat within 24 hours.

2.5 Supply Chain Incident Response Readiness

If supplier assurance processes remain too slow and supply chain visibility incomplete, it is unsurprising that incident response across the supply chain is also often slower than organisations would like. In the 2026 survey, only 6% of respondents said they could accurately map their exposure across their supplier ecosystem in under four hours following a major cyber incident in the supply chain. By contrast, 45% estimated it would take between four and 24 hours, 26% said one to three business days, and 23% said it would take more than a week and would require manual outreach to suppliers.

These are significant delays in a threat environment where major vulnerabilities and supply chain incidents can cascade rapidly. If an organisation cannot quickly determine whether an affected supplier supports an important business service, which systems or processes depend on that supplier, and what exposure may sit further down the chain, then response efforts are immediately hampered. The issue is not simply one of speed only; it is whether current TPRM processes give security and resilience teams enough usable information to make time-sensitive decisions under pressure.

The results suggest that, for many organisations, they still do not. Even where firms have well-established supplier assurance processes, these do not necessarily translate into rapid exposure mapping or confident incident triage when a real-world event occurs. This highlights a core weakness of siloed and point-in-time TPRM: it may generate documentation, but not always provide timely operational insights.

2.6 How Effective is Traditional TPRM in 2026?

Despite the limitations described above, 60.4% of respondents still regard traditional TPRM as at least somewhat effective in reducing supply chain cyber risks, with 27.8% even considering it very effective. Only 5.2% consider it not very effective, and only 0.2% of respondents regard it as entirely ineffective.

These figures demonstrate a further decline in confidence in traditional TPRM from last year, when 37.2% still considered TPRM as very effective. In 2026, as in 2025, the dominant response remains "somewhat effective". Viewed alongside the incident prevalence data — where 82.4% of respondents experienced at least one supply chain incident in the past year — this suggests that most organisations operate with a TPRM function they consider useful but insufficiently effective at markedly reducing supply chain cyber risks. The process thus continues to provide a degree of assurance, but not enough to prevent incidents from occurring at a high and persistent rate.

When asked to identify the single biggest shortcoming with prevailing TPRM approaches, the most frequent response was the lack of visibility into supply chain dependencies beyond direct third parties, cited by 24.8% of respondents.

27.8%

of respondents still regard traditional TPRM as very effective at significantly reducing supply chain cyber risks.

The inability to continuously monitor suppliers' internal security controls came second, selected by 19.8% of respondents. The lack of human and financial resources committed to TPRM came third with 15.4% of respondents providing this as their answer, while 13% cited the lack of collaboration and information sharing with industry peers as the principal shortcoming they see.

2.7 Why Traditional TPRM is No Longer Enough

Taken together, the findings in this section point to a model that remains necessary and partially effective, but increasingly strained and in need of reinvention. Traditional TPRM is still the baseline approach most organisations rely on, and few would argue it should disappear altogether. But the 2026 survey once again establishes that it remains too slow, too manual, too partial in the visibility it affords organisations, and too limited in the operational outcomes it produces.

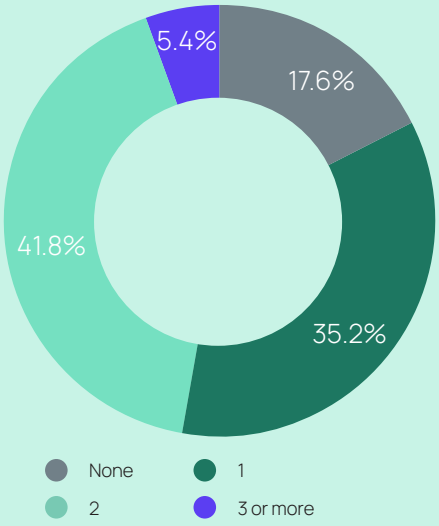
Most importantly, the data suggests that many UK organisations are still trying to manage a fast-moving, deeply interconnected supply chain threat using approaches that were designed for a more static and less interdependent environment. The result is a widening gap between the scale of the threat and the capabilities organisations can bring to bear through traditional TPRM alone.

> "A big challenge with third-party risk management comes down to how corporations and other organisations tackle peer-to-peer communication from within their respective siloes. We (as customers of common suppliers) need to get better at working with each other and trusting what our peers are doing. Using feedback as a form of intelligence about shared interests would allow companies to focus more time on fixing the things we really care about."

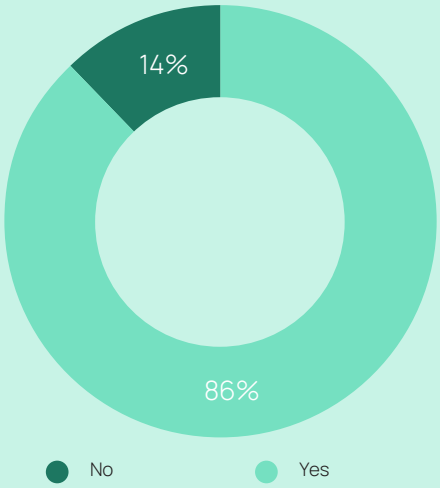
Jay Vinda, Global CISO and Cyber Risk Engineering Lead, Mosaic Insurance

Survey Findings

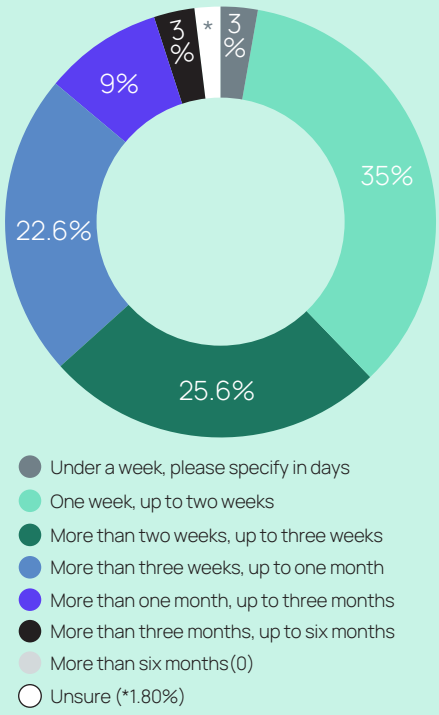
Q1. In the past 12 months, how many cyber security incidents have you experienced in your supply chain?



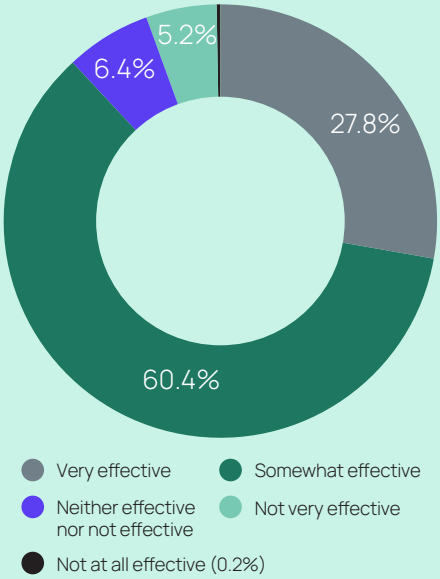
Q2. Do supply chain cyber incidents rank among your top three areas of concern for 2026?



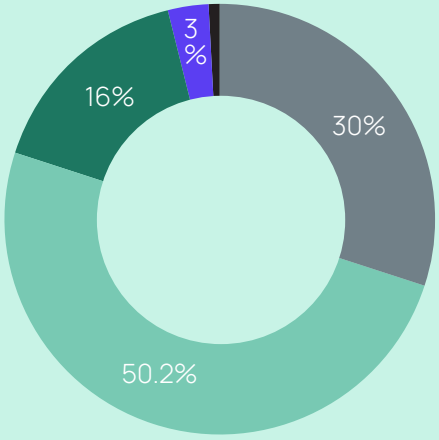
Q3. On average, how many weeks does it take your organisation to complete the security due diligence process for a new supplier?



Q4. How effective, if at all, do you believe traditional TPRM still is in significantly reducing supply chain cyber risks to your organisation in 2026?

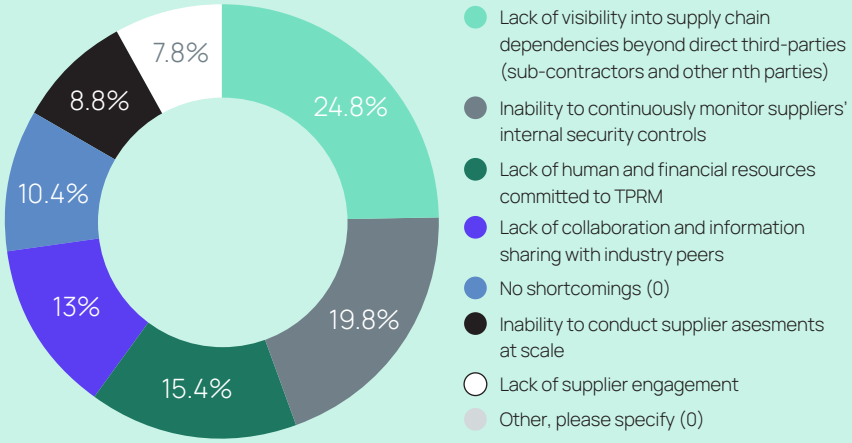


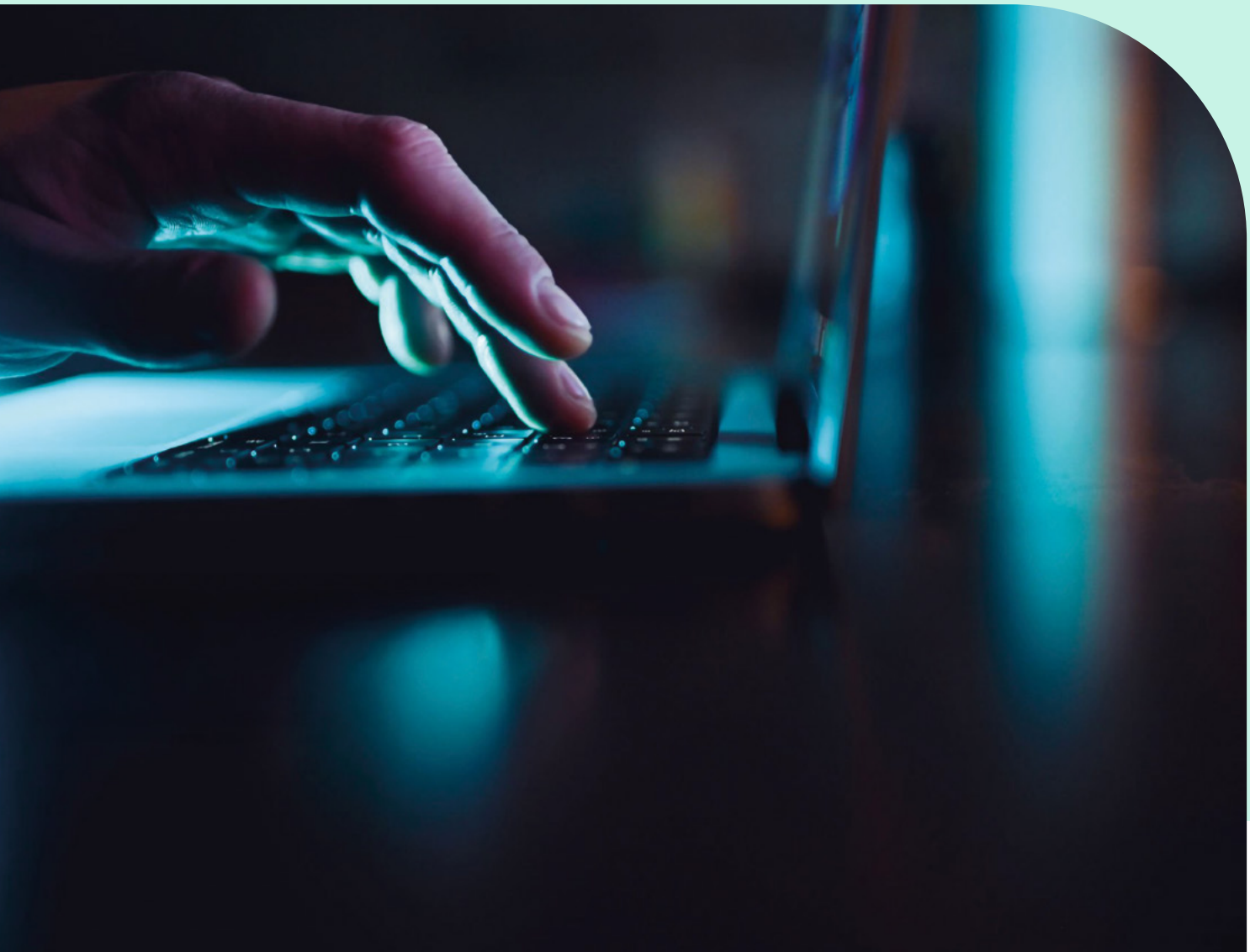
Q5. Beyond your direct suppliers, what level of visibility does your firm have into material sub-contractors (4th, 5th, nth parties)



- **Full visibility:** The entire chain of sub-contractors and sub-contractors of sub-contractors(4th, 5th and nth parties) contributing to your important business functions
- **High visibility:** All sub-contractors (4th parties) of our critical third parties
- **Partial visibility:** Some sub-contractors (4th parties) of our critical third parties
- **No visibility:** No oversight beyond direct critical third parties
- **N/A** (0.60%)

Q7. What, if anything, do you believe to be the single biggest shortcoming or persistent challenge with prevailing approaches to TPRM as a means to reduce risks emanating from your supply chain?





Section 3:
From Third-Party Risk Management to Active Supply Chain Security

3.1 Section Overview

The previous section showed that traditional TPRM remains an essential foundation for managing supplier risk, but also that it continues to struggle with delivering the speed, visibility and operational usefulness required in today's escalating threat environment.

These shortcomings increasingly matter because supply chain risk is no longer just a bilateral issue between one customer and one supplier. The increasing interdependence of digital supply chains means that the security of one organisation is shaped by a much wider ecosystem of subcontractors, shared service providers, cloud platforms and software dependencies. As regulators have recognised, achieving resilience in this environment requires more than repeating the same assessment processes more often. Incremental improvements to questionnaires, review cycles or internal workflows may help at the margins, but they do not resolve the underlying structural weaknesses of traditional TPRM: siloed assessments, limited standardisation, weak visibility across deeper tiers, and a lack of operational integration.

What is needed, therefore, is not simply more TPRM, but a more operational model of supply chain security. Risk Ledger describes this model as Active Supply Chain Security (ASCS): a continuous, network-first approach that connects organisations and suppliers into a living ecosystem of shared visibility and collective defence. This section defines what ASCS is, how it differs from traditional TPRM, and how far UK organisations appear to have progressed toward this model in practice.

The five pillars of Active Supply Chain Security

- Standardised assessment framework
- Continuous monitoring
- Network visibility
- Collective defence
- Faster incident response

3.2 What is Active Supply Chain Security?

At its core, Active Supply Chain Security is an evolution of supplier risk management from a static, compliance-focused activity into a more continuous and operational security discipline. Rather than treating each supplier relationship as an isolated assurance exercise, ASCS starts from the reality that modern supply chains are interconnected ecosystems in which risks, dependencies and incidents often extend well beyond the immediate contractual relationship with direct suppliers.

Whereas traditional TPRM is usually periodic, bilateral and bespoke, where each organisation sends its own questionnaires, conducts its own reviews, and holds only a partial view of supplier risk, ASCS is designed to be ongoing, standardised and network-first. It enables organisations to move from isolated assessments toward a more dynamic understanding of their supply chain exposure.

In that sense, ASCS should not be understood as replacing TPRM, but as building on it. It retains the need for supplier assurance, but seeks to make that assurance more current, more scalable, more comparable, more continuous and more operationally useful in the face of fast-moving threats.

3.3 The Core Features of ASCS

Standardised assessment framework

In many ways, the basis for ASCS is the utilisation of a standardised assessment framework and reusable supplier profile. Instead of every customer asking different questions in different formats, suppliers maintain a single, structured profile that can be shared across multiple client relationships. This reduces duplicated effort, improves comparability between suppliers, and creates a common language of risk. It means that multiple organisations are effectively able to look at the same supplier through a shared lens rather than each starting from scratch. Firms can benchmark a supplier's posture against peers, identify where performance is weakening over time, and share intelligence with partner organisations who are assessing the same supplier.

The efficiency gains of using a shared framework are significant. Onboarding timelines shrink when much of the assurance data already exists on a shared network. Supplier fatigue — the erosion of response quality that occurs when suppliers are completing dozens of overlapping questionnaires for different clients — is reduced. The resources that TPRM teams currently spend on administering bespoke assessment processes can be redirected towards analysis, remediation and response.

Continuous Monitoring

The second feature of ASCS is continuous monitoring. It is, however, important to be precise about what continuous monitoring means in the context of TPRM. External vulnerability scanning — which only assesses publicly visible signals about a supplier's perimeter — is often described as continuous monitoring. It is not, or at least not in full. It provides outside-in exposure data but gives no visibility into the internal security controls that determine a supplier's actual risk posture: access management, staff training, patch management, incident response capability.

ASCS enables more genuine continuous monitoring by combining regular supplier reassessments of their internal security controls, provides real-time updates and control-level change notifications to clients, while external monitoring features add additional objective signals from the supplier’s digital footprint. These include automated asset discovery to identify all relevant domains/subdomains; port scanning of exposed services; and indicators such as misconfigurations or SSL/certificate issues.

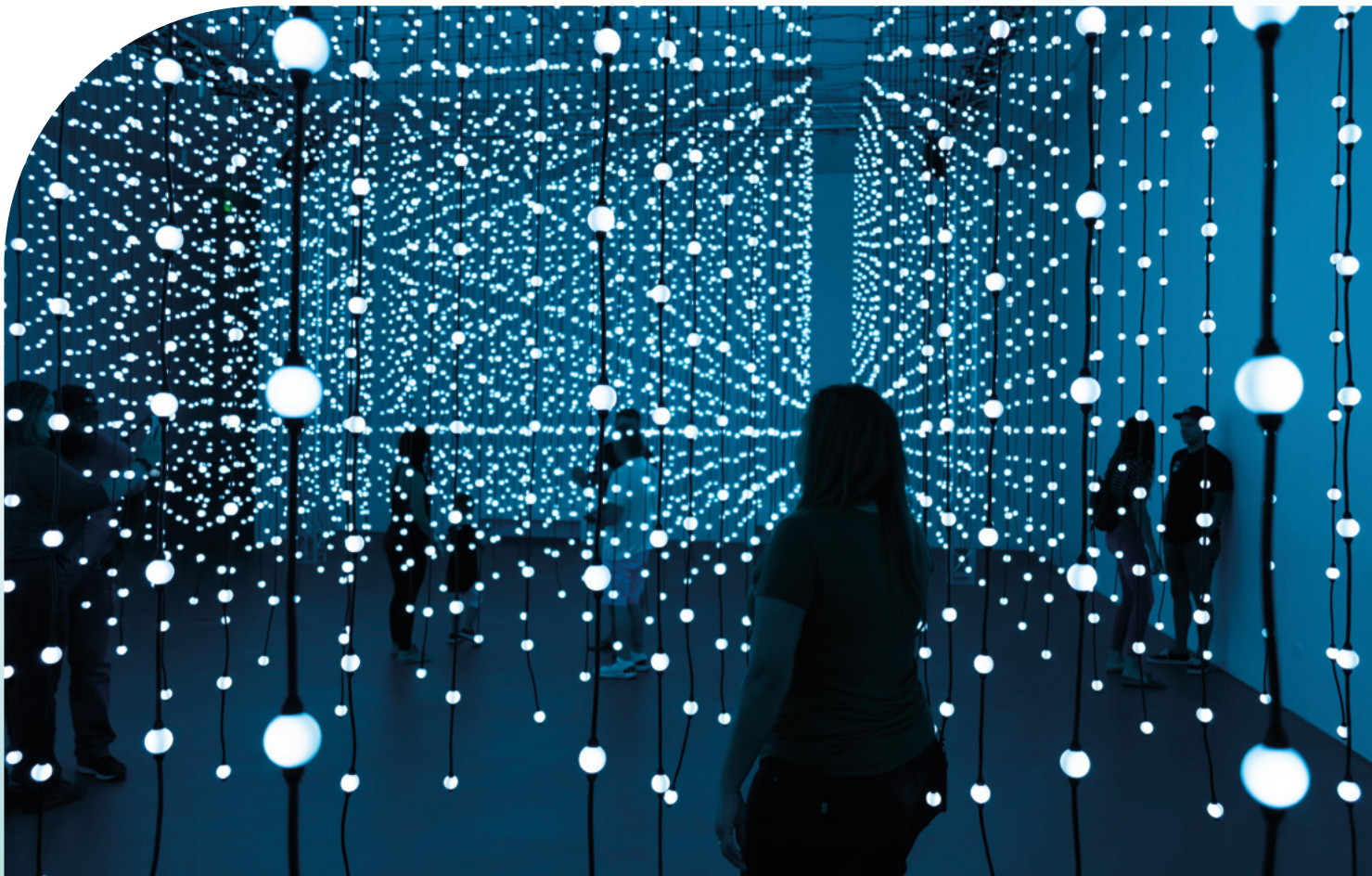
Network visibility

The third ASCS feature is network-level visibility. Because organisations and suppliers sit within a connected ecosystem, ASCS is intended to reveal dependencies not only between direct customers and their suppliers, but also across deeper tiers of the supply chain. This makes it easier to understand which suppliers are shared, where dependencies may cluster, and how disruption could spread through the system.

Collective defence

ASCS is built around a logic of collective defence. The point is not simply to improve the efficiency of individual supplier reviews, but to recognise that supply chain security outcomes improve when organisations have a more shared, structured and operational view of supplier risk, not least on a sectoral level where organisations often share the same suppliers. Organisations that share their own supply chain intelligence with their peers on a common network can, with appropriate governance, overlay their supply chain maps to identify shared dependencies that no single organisation could see alone.

Whereas an individual organisation, however large its TPRM programme, has visibility of its own direct suppliers and, partially, of their subcontractors, what it cannot see is how its supplier relationships overlap with those of ten or twenty other organisations in the same sector. If six of those organisations all share a common fourth-party cloud storage provider, that is a systemic concentration risk for the sector — but it is invisible to each organisation looking only at its own supplier data. Collective mapping changes that. This is how concentration and systemic risks to entire sectors, which regulators are working hard to identify, become easily visible.



Faster incident response

Finally, faster exposure mapping and incident response. ASCS also provides the data architecture that makes rapid exposure mapping possible when incidents occur. When a major supplier is compromised, the first critical question is: which of our business services depend on this supplier, directly or indirectly? With a connected network approach to TPRM that brings organisations and their suppliers and these suppliers' suppliers together on the same platform, it becomes possible to quickly bulk-contact all organisations on the network to ascertain whether they are affected and how they are responding, and notify all their connected clients automatically. This significantly cuts incident triage time from days to hours and allows for a coordinated network-level response. It also provides a view of the potential blast radius of an incident by overlaying emerging threat data onto the existing supply-chain network map.

3.4 Are Organisations Adopting Active Supply Chain Security?

If ASCS represents the direction of travel, the next question is how far UK organisations have actually progressed toward it. The survey suggests that while there is growing awareness of the need for a more operational and collaborative approach, most organisations are still only part-way through the transition.

55.4%

of respondents have insufficient access to the security teams at their critical suppliers.

Direct relationships with supplier security teams remain uneven. Only 43.8% of respondents said their TPRM function has established relationships with the security teams at most of their critical suppliers, while 53% said they have such access, but only to some critical suppliers and 2.4% stated that they don't at all. This matters because a more operational model depends on direct engagement with the people who can clarify controls, discuss remediation and respond quickly during incidents.

Continuous assurance also remains immature. Just 40.6% of respondents described their capability to monitor the internal security controls of important suppliers as fully automated and real-time, while 53.6% said it was partially automated with quarterly or event-triggered updates. Meanwhile, 3.8%, still relies on manual or static annual spreadsheet-based assessments, and 1.6% described their approach as ad hoc and reactive. Despite growing recognition of the need for more dynamic oversight, genuine continuous supplier assurance therefore remains elusive for the majority of organisations.

53.6%

of respondents described their ability to continuously monitor the internal security controls of critical suppliers as partially automated with quarterly or event-triggered updates.

There are, however, strong signs that the market is receptive to a more networked and collaborative model. When asked about support for an industry-wide collaborative model in which supplier intelligence and assurance data are shared with peers, 42% said their firm would be very supportive and 50.2% said they would be somewhat supportive. Only 0.6% were somewhat unsupportive. This indicates substantial openness to more standardised and collective approaches, even if practical implementation remains limited.

3.5 The Shift to Network-Level Supply Chain Security

Taken together, these findings point to the need for a broader transition in how supply chain security is understood and practised. Moving toward network-level security offers several clear benefits. It can reduce duplicated effort through standardisation and significantly speed up onboarding and assessment times, improve supplier engagement by lowering assessment burden, provide better visibility into dependencies beyond direct suppliers, and support faster, more informed responses when incidents occur. Most importantly, it aligns supply chain security more closely with the realities of operational resilience where resilience depends not only on the controls of individual firms, but on the health and visibility of the wider ecosystem they depend on.

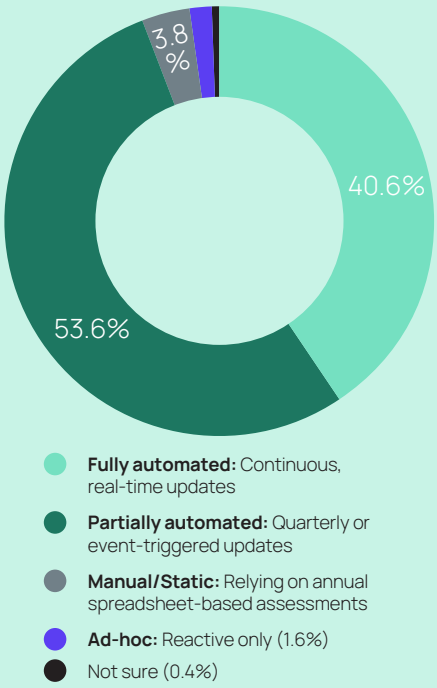
This is the central argument of the section. The challenge facing UK organisations is no longer simply how to perform TPRM more efficiently, but how to evolve from isolated, point-in-time supplier assurance toward a more continuous, operational and network-aware model of collective defence. The next section turns from concept to practice, examining how organisations and communities across the UK are already beginning to make that transition and what the benefits look like in the real world.

93.2%

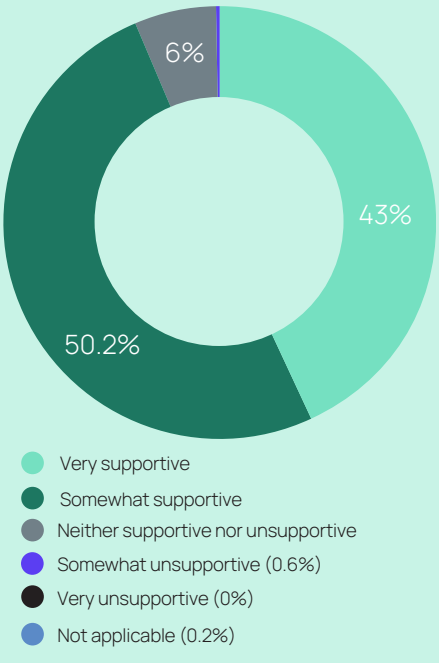
of respondents would be supportive of greater collaboration with industry peers.

Survey Findings

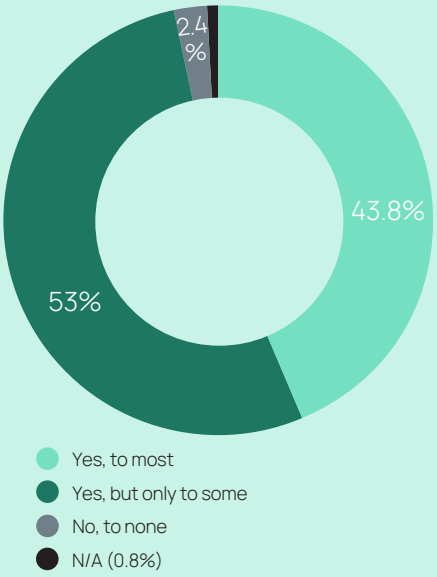
Q8. How, if at all, would you describe your firm's current capability to continuously monitor the internal security controls of your important third parties (i.e. direct suppliers)?



Q9. How supportive or not supportive would your firm be for an industry-wide collaborative model, where supplier intelligence and assurance data are shared with your peers?



Q10. Does your TPRM function have relationships (direct access) with the security teams at all your critical suppliers?



Section 4: Active Supply Chain Security in Practice

4.1 Section Overview

As discussed in previous sections of this report, regulators are no longer just concerned with the resilience of individual firms, but with the identification of shared dependencies and potential systemic single points of failure across entire sectors. As also argued, traditional bilateral TPRM cannot solve that problem on its own, because an individual organisation cannot see how its own supplier relationships overlap with those of peers in the same sector. That is precisely what is required to move from individual resilience to sectoral resilience in practice. Once organisations collaborate on a shared network, however, and work from a more standardised supplier assessment model, risks that remain invisible in isolation begin to come into view.

4.2 Collective Defence Through Supply Chain Security Communities

Across the UK's most critical sectors, organisations are already embracing this new model of collective defence. By leveraging Risk Ledger's collaborative supply chain security platform, organisations can now join forces with their industry peers to securely share their respective supply chain maps, best practices, and supply chain risk intelligence. Given their often significantly overlapping supply chains, doing so enables them to map complex supplier relationships, far beyond immediate third-parties, and coordinate risk mitigation efforts while reducing the burden on both these organisations and their suppliers.

Key benefits of this community model:

- **Share supplier assessments and risk data:** Reducing duplication and improving the quality and consistency of risk information.
- **Map extended supply chain dependencies:** Visualising not just direct suppliers, but also fourth- and fifth-party relationships, and identifying shared dependencies and single points of failure.
- **Detect and respond to systemic risks:** By aggregating data across multiple organisations, Risk Ledger can highlight vulnerabilities that have the potential to impact entire sectors, enabling proactive, coordinated responses.
- **Support regulatory compliance:** By providing industry-wide visibility and audit trails, the platform helps organisations and regulators meet the requirements of new operational resilience and cyber regulations.
- **Increase incident response speeds:** The ability to collaboratively triage, prioritise, and mitigate risks during times of emerging threats.

We will now look at three such communities across the UK public and private sectors and their experiences and insights.

4.3 UK Government Bodies Defend-as-One

According to the National Audit Office (2025), "the threat government faces from cyber attack is rapidly evolving and is the most sophisticated it has ever been." As the government is currently introducing the Cyber Security and Resilience Bill to regulate critical sectors, it is determined to ensure it also holds public sector bodies to equivalent or even higher standards. In pursuit of this goal and to provide centralised visibility of where systemic risk lies and identify opportunities for standardising and improving government-wide supply chain risk processes, 26 government clients are using the Risk Ledger platform to harden their individual and sectoral resilience.

Findings:

Collectively, these 26 organisations have connected with 3,240 of their direct third parties on the platform. Through these supplier connections, the platform was able to identify another 5,886 dependencies across this community's shared nth parties, including:

Supply Chain Depth

3rd Parties	4th Parties	5th Parties	6th Parties	7th Parties	8th Parties
3,240	2,331	2,393	1,086	74	2

The platform was also able to identify 1,264 potential concentration risks across these nth parties with the following number at third and fourth party levels:

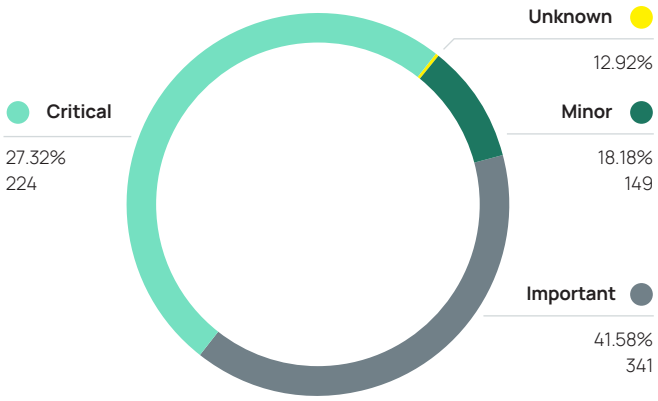
Total Concentration Risks

Total	3rd Parties	4th Parties
1,264	820	354

Crucially, out of these 820 concentration risks at the third party level, 224 are rated 'critical', meaning an incident at a supplier is likely to disrupt essential services at multiple public sector organisations at once.

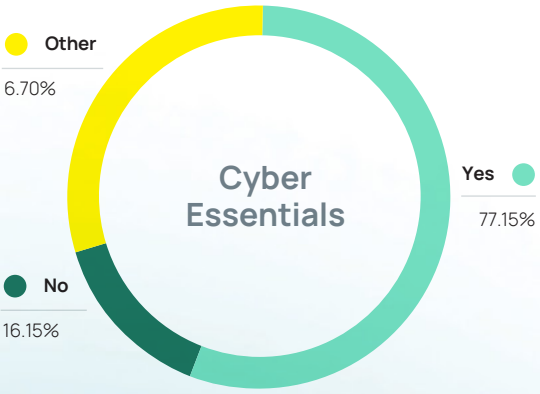
> "Risk Ledger's Network Visualisation Tool has enabled us to efficiently identify critical risks across our supply chain, helping us address potential concentration risks before they escalate."
>
> **Chris Phillips,** Third-Party Compliance and Assurance Lead, Home Office Cyber Security (HOCS) | Governance, Risk and Compliance (GRC)

Third-Party Concentration Risks by Criticality

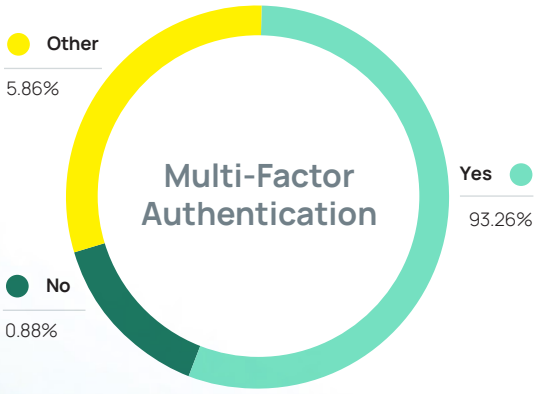


What also emerged from this network visualisation and data analysis was that out of the 224 potential concentration risks at the third party level that were classified as critical, 36 suppliers did not have a Cyber Essentials certification in place, 2 were not using Multi-Factor Authentication (MFA) for securing remote access to their network or cloud environments, and 15 did not regularly test or rehearse their Business Continuity and Disaster Recovery plans.

Potential concentration risks with control weaknesses



16.15% of suppliers are not Cyber Essential certified



0.88% of suppliers are not using Multi-Factor Authentication (MFA)for securing remote access to their network or cloud environments

6.7% of suppliers do not regularly test or rehearse their Business Continuity and Disaster Recovery plan

4.4 Local Authorities Defend-as-One

Today, local authorities face a plethora of rising supply chain threats and systemic fragility. Our 2026 survey found that 88% of UK councils experienced at least one supply chain cyber incident in the past year alone. Contributing factors that UK councils in particular are faced with often include fragmented, outdated IT infrastructures, limited financial resources, and a shortage of skilled cyber security personnel.

Recognising that no council can secure its supply chain in isolation, a group of 25 UK councils, supported by regional WARPs across Scotland, England and Wales, came together and partnered with Risk Ledger to transition from manual, siloed processes to a collaborative "Defend-as-One" model. This shift towards a new and more collaborative model of TPRM brought immediate benefits and insights.

Findings:

Collectively, these 25 organisations have connected with 1,004 of their direct third parties on the platform. Through these supplier connections, the platform was able to identify another 7,659 additional dependencies across this community's shared nth parties, including:

Supply Chain Depth

3rd Parties	4th Parties	5th Parties	6th Parties	7th Parties	8th Parties
1,004	1,599	1,506	929	2,518	1,107

The platform was also able to identify 1,240 potential concentration risks across these nth parties with the following number at third and fourth party levels:

Total Concentration Risks

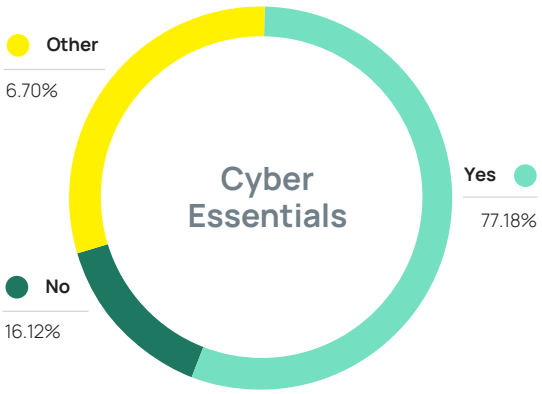
Total	3rd Parties	4th Parties
1,240	364	414

Crucially, out of these 364 concentration risks at the third party level, 99 are rated 'critical', meaning an incident at a supplier is likely to disrupt essential services at multiple local authorities at once.

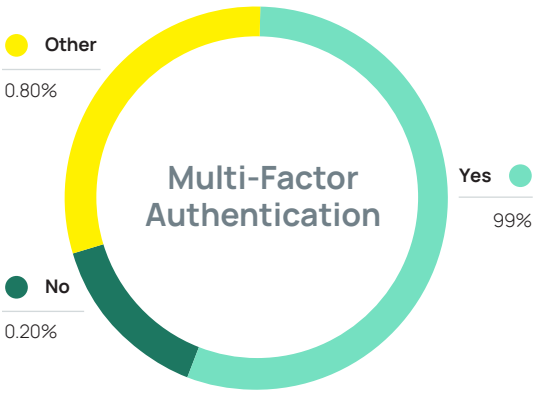
Third-Party Concentration Risks by Criticality

What also emerged from this network visualisation and data analysis was that out of the 99 potential concentration risks at the third party level that were classified as critical, 13 suppliers did not have a Cyber Essentials certification in place, 1 was not using Multi-Factor Authentication (MFA) for securing remote access to their network or cloud environments, and 4 did not regularly test or rehearse their Business Continuity and Disaster Recovery plans.

Potential concentration risks with control weaknesses



3.5% of suppliers are not Cyber Essential certified



0.2% of suppliers are not using Multi-Factor Authentication (MFA)for securing remote access to their network or cloud environments

1% of suppliers do not regularly test or rehearse their Business Continuity and Disaster Recovery plan

4.5 Financial Services Defend-as-One

A group of 30 UK financial institutions established a collaborative community of peers to enhance sector-level operational resilience, identify shared concentration risks, and accelerate their ability to respond to emerging threats. Driven by the execution mandates of DORA and the UK operational resilience framework, the primary objectives of the participants included gaining comprehensive visibility into the extended sub-tier dependencies supporting their important business services. Joining this collective network also allows these firms to identify and mitigate systemic single points of failure across their shared supply chains, align technical remediation plans, and deploy the automated mapping capabilities required to mitigate exposure during active ecosystem breaches.

Findings:

Collectively, these 30 organisations have connected with 2,780 of their direct third parties on the platform. Through these supplier connections, the platform was able to identify another 6,529 additional dependencies across this community's shared nth parties, including:

Supply Chain Depth

3rd Parties	4th Parties	5th Parties	6th Parties	7th Parties	8th Parties
2,780	1,161	1,769	2,814	714	71

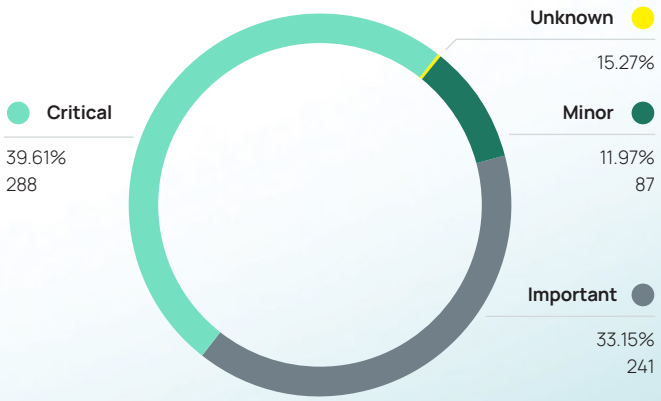
The platform was also able to identify 1,322 potential concentration risks across these nth parties with the following number at third and fourth party levels:

Total Concentration Risks

Total	3rd Parties	4th Parties
1,322	727	235

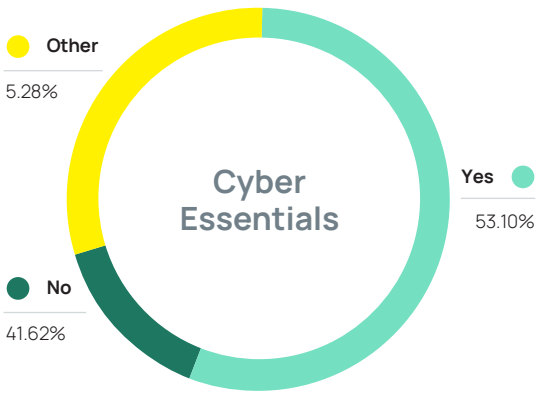
Crucially, out of these 727 concentration risks at the third party level, 288 are rated 'critical', meaning an incident at a supplier is likely to disrupt essential services at multiple financial institutions at once.

Third-Party Concentration Risks by Criticality

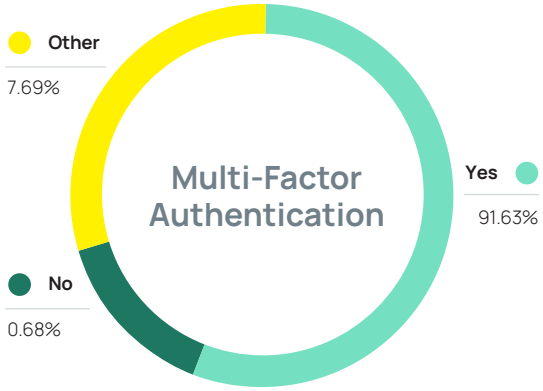


What also emerged from this network visualisation and data analysis was that out of the 288 potential concentration risks at the third party level that were classified as critical, 120 suppliers did not have a Cyber Essentials certification in place, 2 were not using Multi-Factor Authentication (MFA) for securing remote access to their network or cloud environments, and 10 did not regularly test or rehearse their Business Continuity and Disaster Recovery plans.

Potential concentration risks with control weaknesses



4.1% of suppliers are not Cyber Essential certified



0.6% of suppliers are not using Multi-Factor Authentication (MFA)for securing remote access to their network or cloud environments

3.4% of suppliers do not regularly test or rehearse their Business Continuity and Disaster Recovery plan

4.6 What These Examples Show

These examples offer a glimpse into the practical expression of how organisations are already actively working to institute the two interlinked pivots discussed in this report: the move away from reactive, assessment-led TPRM towards a more active and operational model of supply chain security. The second is the move beyond the resilience of the individual organisation toward forms of shared visibility and collaboration that support resilience at sector level.

The findings from these three communities of peers highlight the scale and complexity of the challenge facing such crucial sectors as government, local authorities, and financial services. They demonstrate that systemic concentration risks cannot be identified in isolation. Only through collaboration can institutions gain the visibility required to uncover shared dependencies and better understand the interconnected nature of their supply chains. This level of insight is essential to building more informed and cyber resilient sectors across the UK.

The data also highlighted further risk factors deserving attention. It revealed, for example, that numerous suppliers that could pose concentration risks to these three communities of peers and were classified as critical did not possess Cyber Essentials certification, did not enforce Multi-Factor Authentication for securing remote access to their organisations' network or cloud environments, or did not regularly test or rehearse their Business Continuity and Disaster Recovery plans. By offering a clear view of the participants' extended supply chain, this allows community participants to identify those suppliers that initial risk mitigation efforts could concentrate on.

An Example of a Community Network Map on Risk Ledger

Conclusion: Securing the UK's Digital Supply Chain

This report describes a reality where the problem with managing supply chain cyber risk has been recognised for several years, but which has not yet led to a fundamental re-engineering of the prevailing model for supply chain risk management to match the pace and depth the new environment requires. Supply chain incidents remain widespread in 2026: 82.4% of surveyed organisations experienced at least one in the past year alone, and almost half reported two or more. Threat actors are increasingly sophisticated, often state-linked, and deliberate in their use of supplier relationships as a route into critical services and infrastructure. Yet, most organisations still manage supply chain risk using processes designed for a more static and less interconnected world.

The 2026 survey findings are clear about where the gaps are largest. Only 8.8% of respondents can map their exposure across their supplier ecosystem in under four hours when a major incident occurs; more than half require more than a day. Most still rely on only periodic assessments that leave them without current information on supplier security postures in between assessment cycles, while 55.4% of TPRM functions only have some or no direct access to and established relationships with the security teams at their direct suppliers, limiting their ability to respond swiftly and effectively when supply chain incidents do occur. As Section 2 argued, these are not marginal weaknesses; they are symptoms of a model that generates documentation but does not reliably produce timely, operationally-actionable and readily-available insights.

The findings also reflect the structural limitations of traditional TPRM despite the improvements we could witness in 2026: bilateral, compliance-oriented, and focused on the firm–supplier relationship in isolation. The model was not designed to reveal how dependencies cluster across sectors, or to support the kind of rapid, data-driven exposure mapping that today's threat landscape and regulatory expectations necessitate.

The evidence from organisations that have begun to operate differently points to a more constructive path forward than to simply attempt to optimise current approaches. The experiences of the community examples on Risk Ledger described in Section 4 — government, local authorities and financial institutions — show that collective supply-chain mapping is feasible, that it produces a far richer picture of dependencies and concentration risks than any single organisation can generate alone, and that the collaboration required to make it work is already happening in practice. The regulatory direction outlined in Section 1 reinforces this trajectory. The new cyber security and operational resilience rules in the EU and UK all point towards the need for greater sector-level visibility.

Active Supply Chain Security — standardised assessments, more continuous insight into internal controls, collaborative dependency mapping and closer integration with operational security — provides a practical way of building those capabilities. As this report has argued, it offers a different way of organising supply chain security so that it can operate at the speed, scale and depth the UK's digital economy now demands.

Appendix

Survey Methodology

This report draws on a robust, mixed-methods approach combining authoritative open-source data, a targeted survey of UK cyber security professionals, and empirical insights from Risk Ledger's platform data.

Data sources

Open-source Data

We analysed publicly available, authoritative sources including ENISA, the World Economic Forum and UK government publications to contextualise supply chain cyber security trends and regulatory developments.

Survey of UK Cyber Security Professionals

Conducted by Censuswide, the survey gathered 500 responses from professionals actively involved in cyber security and Third Party Risk Management across diverse UK sectors. The sample was carefully scoped and quota-controlled to ensure representation across industries (including financial services, healthcare, government, energy, police, and others) and organisation sizes, with a minimum of 50 respondents per qualifying sector.

The survey targeted individuals with varying levels of involvement in their organisation's cyber security and third party risk management strategies, including senior decision-makers (CISOs, Heads of TPRM, Security Directors) and critical operational staff. Key demographic and role-based screening questions ensured relevance and quality of responses.

Platform Data Analysis

Complementing the survey, Risk Ledger's proprietary platform data was analysed to identify supply chain dependencies up to the 8th tier within communities of peer organisations. This enabled detection of systemic concentration risks and mapping of complex interdependencies that are often invisible to individual organisations.

Risk Ledger Ltd.
Adam House
7-10 Adam Street
London WC2N 6AA
United Kingdom

Company registration number (England & Wales): 10831970

Contact: www.riskledger.com | marketing@riskledger.com