RISK LEDGER

How UK Local Authorities Have Come Together to Secure Public Sector Supply Chains

A Risk Ledger Special Report

About Risk Ledger

Risk Ledger was founded in 2018 by Haydn Brooks and Daniel Saul with a mission to shift the way organisations approach cyber security and risk management in the supply chain by building a global network of connected organisations. Today, Risk Ledger is the cutting-edge Third-Party Risk Management (TPRM) platform, dedicated to transforming supply chain security. We empower security and procurement teams to Defend-as-One, visualising their entire supply chain in real-time and providing unmatched transparency and collaboration. Our platform offers comprehensive, continuously updated risk assessments that reduce compliance burdens and enhance your organisation's cyber defences. By visualising and managing every link in your supply chain, Risk Ledger ensures you are always one step ahead of emerging threats.

Our commitment to asking the right questions and working closely with industry experts allows us to build a more secure, resilient future for all. With our Defend-as-One approach, we strengthen your organisation's ability to detect, respond to, and prevent cyber attacks. Risk Ledger isn't just about managing risk — it's about fortifying your entire supply chain because every link matters in cyber security. We're here to help you secure today's operations and safeguard tomorrow's reputation, creating a safer digital landscape for all.

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

Company registration number (England & Wales): 10831970

Contact: www.riskledger.com I marketing@riskledger.com I +44 1234 567890

Contents

Introduction

Local authorities in the United Kingdom play an indispensable role in public life, providing essential services that frequently involve the collection, storage, and processing of sensitive citizen data. Over recent years, they have accelerated their digital transformation to improve service delivery, and as such are relying on more and more external third-party suppliers and service providers. This growing dependence, however, has also heightened their vulnerability to supply chain cyber threats. Compounding this threat landscape are structural constraints including limited financial resources, skills shortages, and mounting regulatory demands.

Recognising that no local authority could secure its supply chain in isolation, a collaborative model has emerged among UK local authorities, one that harnesses pooled supplier intelligence, shared capabilities, and collective resilience. This Risk Ledger special report explores the underlying challenges faced by local authorities in protecting their supply chains, and how a group of UK councils, several Warning, Advice and Reporting Points (WARPs) and supply chain risk management platform Risk Ledger have come together to Defend-as-One against supply chain threats. We will demonstrate how this unique partnership transforms Third-Party Risk Management (TPRM) from a manual, siloed task into a collective, active cyber defence discipline, establishing a new, forward-looking security standard for the public sector and beyond.

Section 1:
The Situation: The Growing Cyber Threat Facing UK Local Authorities

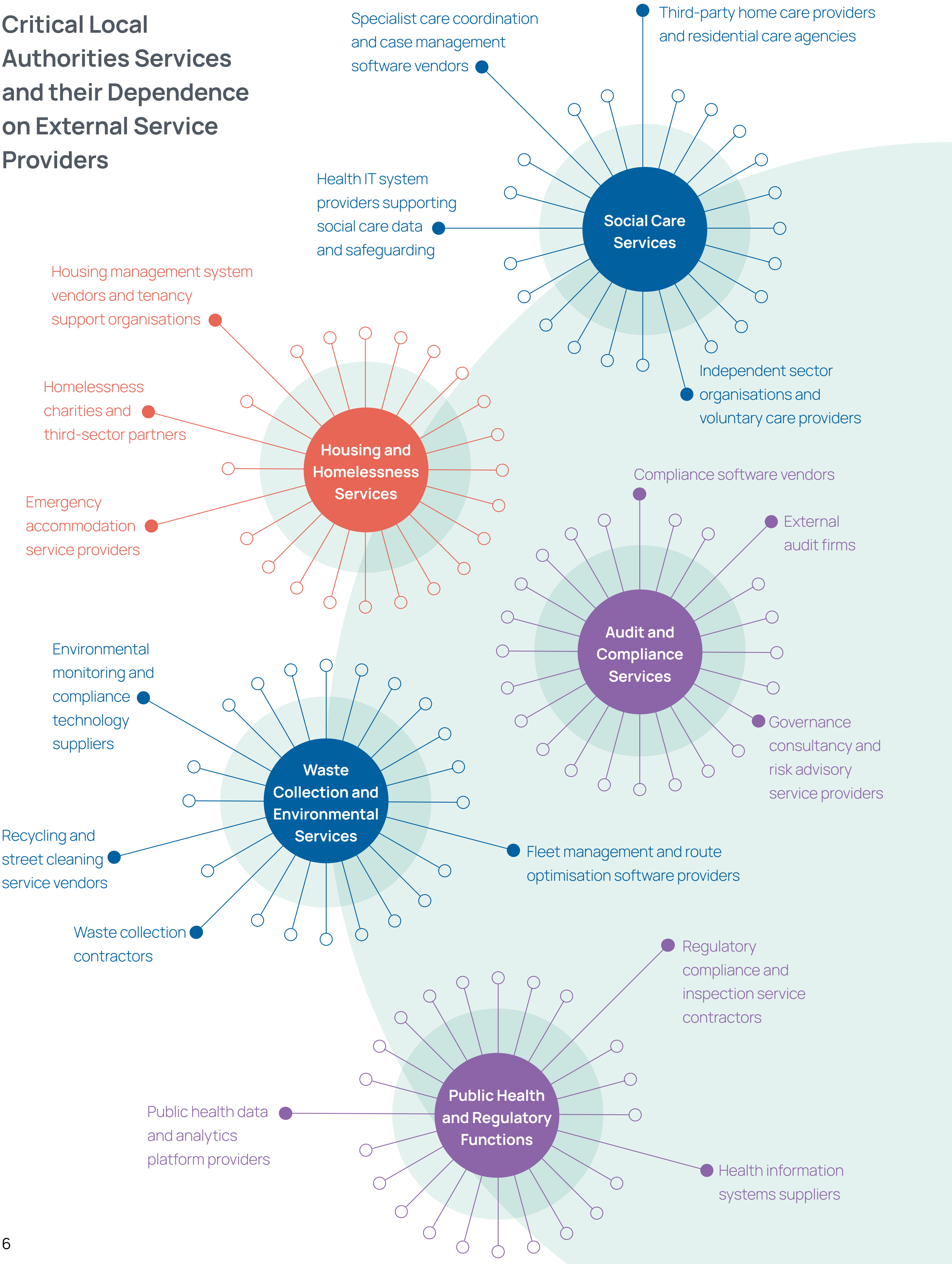
As attackers increasingly target public sector supply chains, UK local authorities have found themselves in the crosshairs. They have become fertile targets for cyber adversaries due to the valuable data they hold and the essential public services they deliver. They are custodians of extensive personal information encompassing social care records, financial data, healthcare details, and more. These datasets represent a treasure trove for criminal actors intent on ransomware, fraud, or identity theft. Their responsibilities also encompass a vast range of services, each potentially exposed through disparate legacy systems and numerous third-party suppliers contributing to these critical functions.

The threat is exacerbated by several systemic factors. Local authorities, due to their often fragmented and outdated IT infrastructures, represent easier targets compared to better-resourced private-sector organisations or larger government agencies. Moreover, the public sector cyber landscape is heavily politicised as a result of a rapidly deteriorating geopolitical environment. Nation-state threat actors, motivated by political or geopolitical objectives, have increasingly shifted their attention to the local government sector, perceiving local authorities as strategic nodes whose disruption can have far-reaching effects on public confidence and governance.

86%

of UK Local Authorities experienced at least one cyber incident in their supply chain in the past year alone.

Critical Local Authorities Services and their Dependence on External Service Providers



Social Care Services

Specialist care coordination and case management software vendors

Third-party home care providers and residential care agencies

Health IT system providers supporting social care data and safeguarding

Independent sector organisations and voluntary care providers

Housing and Homelessness Services

Housing management system vendors and tenancy support organisations

Homelessness charities and third-sector partners

Emergency accommodation service providers

Audit and Compliance Services

Compliance software vendors

External audit firms

Governance consultancy and risk advisory service providers

Waste Collection and Environmental Services

Environmental monitoring and compliance technology suppliers

Recycling and street cleaning service vendors

Waste collection contractors

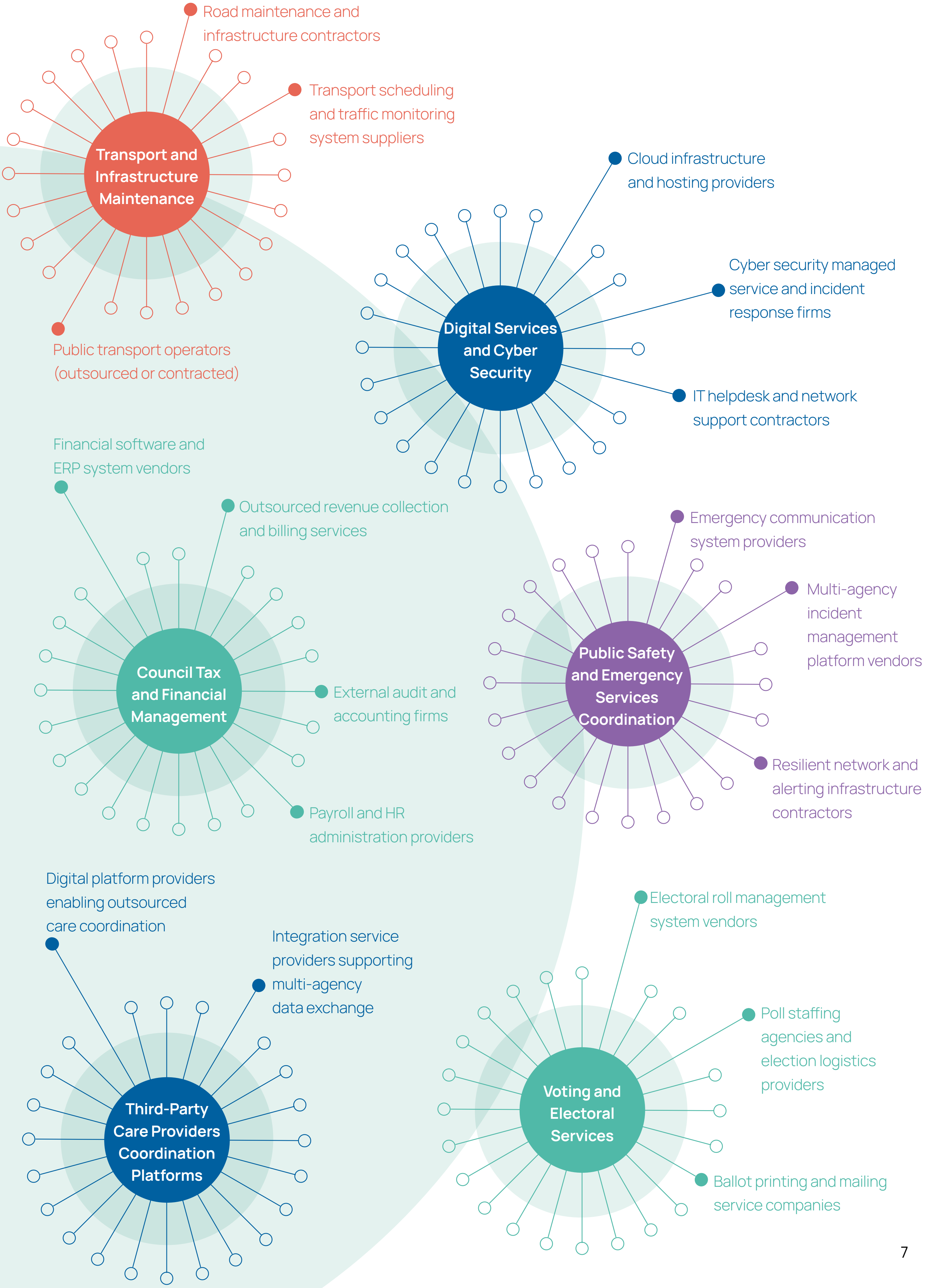
Fleet management and route optimisation software providers

Public Health and Regulatory Functions

Regulatory compliance and inspection service contractors

Public health data and analytics platform providers

Health information systems suppliers



Transport and Infrastructure Maintenance

Road maintenance and infrastructure contractors

Transport scheduling and traffic monitoring system suppliers

Public transport operators (outsourced or contracted)

Digital Services and Cyber Security

Cloud infrastructure and hosting providers

Cyber security managed service and incident response firms

IT helpdesk and network support contractors

Council Tax and Financial Management

Financial software and ERP system vendors

Outsourced revenue collection and billing services

External audit and accounting firms

Payroll and HR administration providers

Public Safety and Emergency Services Coordination

Emergency communication system providers

Multi-agency incident management platform vendors

Resilient network and alerting infrastructure contractors

Third-Party Care Providers Coordination Platforms

Digital platform providers enabling outsourced care coordination

Integration service providers supporting multi-agency data exchange

Voting and Electoral Services

Electoral roll management system vendors

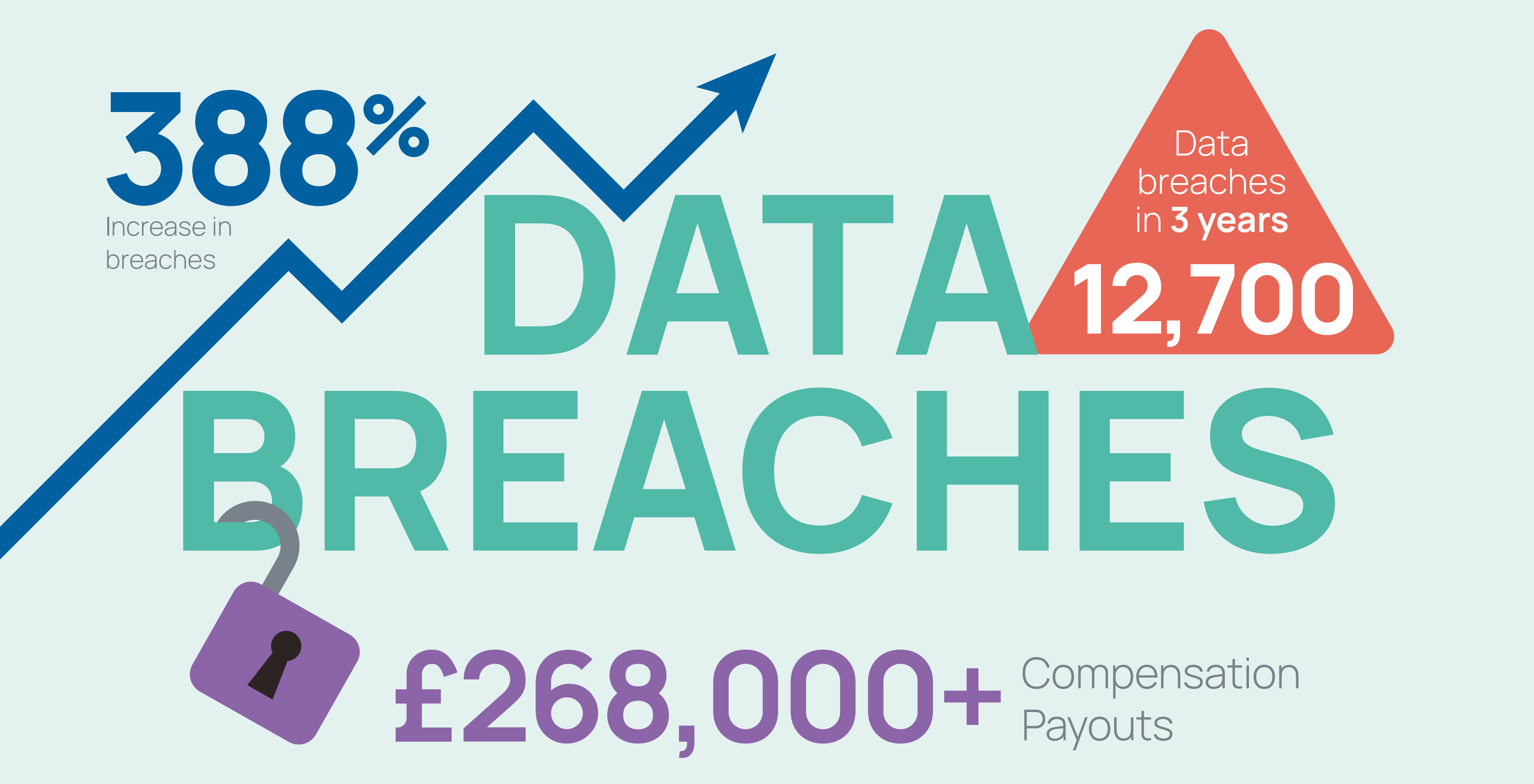
Poll staffing agencies and election logistics providers

Ballot printing and mailing service companies

Data from the past few years paints a concerning picture. Local authorities have witnessed a dramatic rise in cyber security breaches. Recent industry research conducted by Risk Ledger found that 86% of UK local authorities experienced at least one cyber incident in their supply chain in the past year alone, while 48% experienced two or more incidents. Official investigations and Freedom of Information requests revealed that UK metropolitan local authorities alone reported over 12,700 data breaches in the preceding three years, a 388% increase compared to previous periods, with compensation payouts exceeding £268,000. Sheffield City Council recorded more than 1,500 breaches, an indicator of the scale and frequency of attacks.

Similar stories from other local authorities demonstrate that this is a widespread challenge rather than representing isolated incidents. The consequences of these breaches are profound, involving impacting citizen trust, disrupted service delivery, and expensive remediation efforts.

This rising threat of supply chain attacks in particular emerges against a backdrop of severe resource constraints. Despite the increasing risk, local authorities' resources have not scaled enough to build more robust cyber security programmes. Compounded by austerity measures and financial pressures, they thus have limited capacity both in terms of budget and skilled personnel to comprehensively fortify their digital infrastructure and build resilience. As a result, local authorities face an environment where they are expected to manage rising cyber risks, meet increasingly rigorous and comprehensive regulatory requirements, and maintain essential services, all with diminishing resources.



UK Local Authorities in the Cross-hairs: The Case of Glasgow City Council

What happened:

In June 2025, malicious activity was detected on servers managed by a third-party supplier to the council's main ICT provider, CGI. The attack was attributed to a supply chain vulnerability involving this third-party contractor. The council has been working with Police Scotland, the Scottish Cyber Coordination Centre (SC3), and the UK National Cyber Security Centre (NCSC) to investigate the attack.

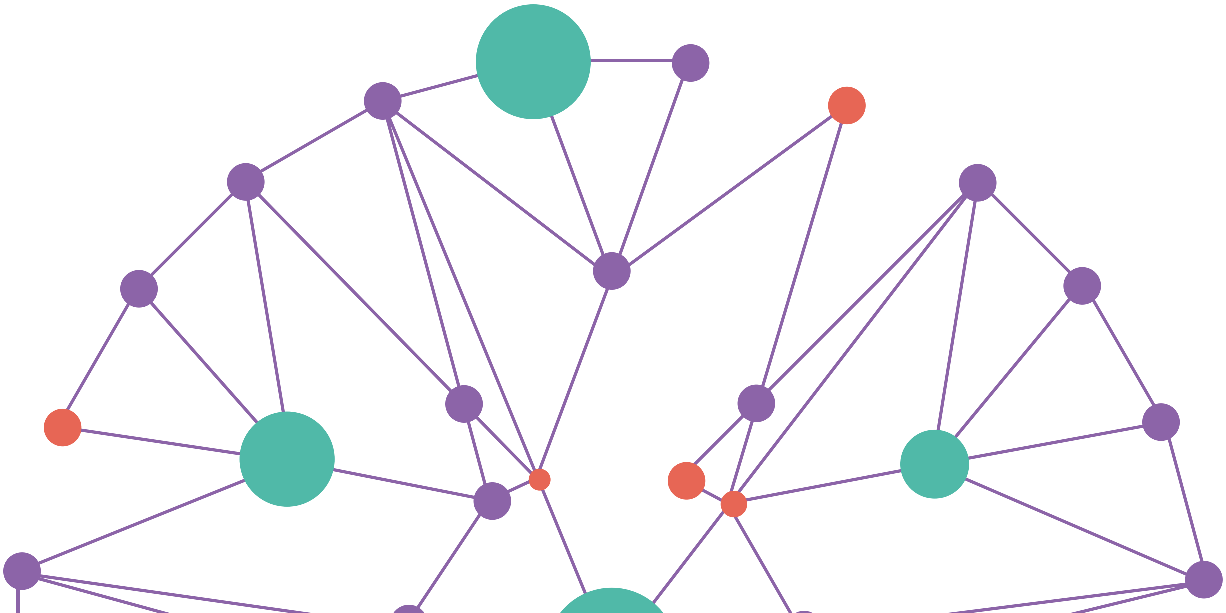
What was the fallout:

The disruption affected both residents' ability to access services and internal council operations. North Lanarkshire Council was also affected due to its reliance on Glasgow for parking fine processing. The council advised users to be cautious regarding phishing attempts and emphasised that financial information was safe as no banking systems were compromised.

Impact:

The attack disrupted numerous council services that relied on these servers. Importantly, no financial systems were compromised, but affected systems included:

- Online planning application access and enforcement
- Penalty charge notices (parking fines) and appeals
- Strathclyde Pension Fund online portal
- Registrar appointment booking
- Revenues and benefits callback appointments
- Various online forms including FOI requests, complaints, bin calendars, pupil absence reporting, and election-related forms.



Section 2: Government Strategy & The Changing Regulatory Landscape

The regulatory landscape in the UK is also fast evolving, with a range of new cyber security and operational resilience rules, from the Bank of England's, Prudential Regulation Authority's and Financial Conduct Authority's Operational Resilience regime, the just published, upcoming Cyber Security and Resilience Bill, or government initiatives such as the UK Government Cyber Security Strategy and related NCSC Cyber Assessment Framework (CAF). What all these new regulations and initiatives share in common is their strong emphasis on supply chain cyber risk.

While UK local authorities are not directly subject to central government cyber regulations, they are working closely with the Ministry for Housing, Communities and Local Government (MHCLG) to align with the Cyber Assessment Framework (CAF) for local authorities and strengthen their cyber resilience, governance, and best practices. The CAF is the UK's high-level blueprint of 14 security principles covering governance, protection, detection, and recovery, designed to ensure resilience in critical services. A pilot programme by MHCLG, running since at least 2023, is creating the Local Government CAF (LG CAF), a tailored, risk-based blueprint to help local authorities with their distinct structures and resource constraints assess and improve cyber resilience across critical systems. MHCLG aims to roll out LG CAF across all local authorities, implementing self-assurance and external verification reporting models.

Identifying Concentration and Systemic Risks to Enhance Sectoral Resilience

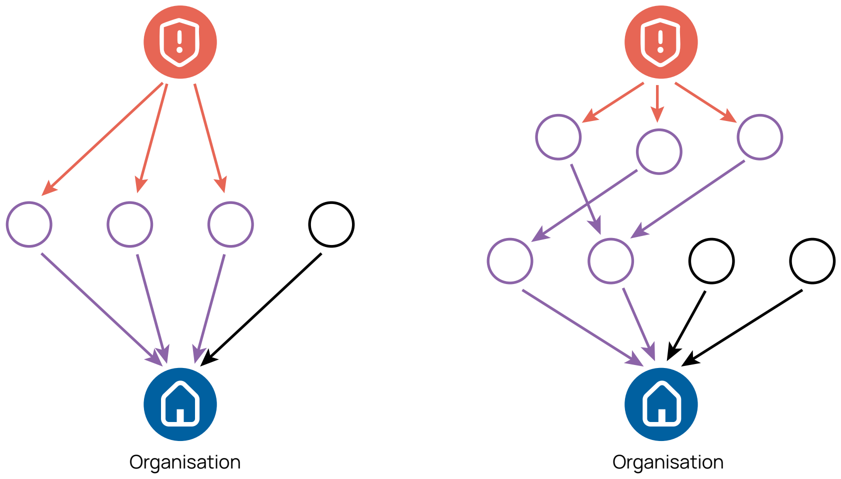
Boosting overall sectoral resilience is an increasing priority for regulators in general, with supply chain security as a key focus. Today's supply chains are highly complex and interdependent, with third-party suppliers also relying on their own suppliers, and so on. Regulators recognise how suppliers anywhere in this vast ecosystem of dependencies could quietly serve dozens of public sector bodies, even if indirectly, potentially amplifying the effects of any disruption or even trigger a cascade across an entire sector.

Thus, a key focus when it comes to supply chain security and resilience in government strategy and guidance is the fundamental importance of attaining enhanced visibility into supply chain dependencies beyond immediate 3rd parties, into 4th, 5th and nth parties. In the words of the GCSS, in order to achieve greater resilience and enhanced supply chain security, "visibility is the foundation from which an accurate assessment of risk can be derived", and only an "improved understanding of suppliers and their dependencies will…enable government to better respond to cyber security incidents that emanate from the supply chain." This is particularly important since, like in many other sectors, critical suppliers to local authorities rely heavily on 'hyperscalers' such as large cloud providers, and as recent incidents have shown, should such hyperscalers experience outages, numerous critical suppliers could be impacted at the same time.

Implicit in the GCSS and many other new regulations is thus the desire of regulators and the government to identify shared systemic and concentration risks, which would be impossible for individual entities to do. It is these dependencies that can introduce potential single points of failure, i.e. when a disruption at this supplier could cascade rapidly, impacting operations far beyond the immediate contractual relationship.

Different types of concentration risks

Individual Concentration Risks

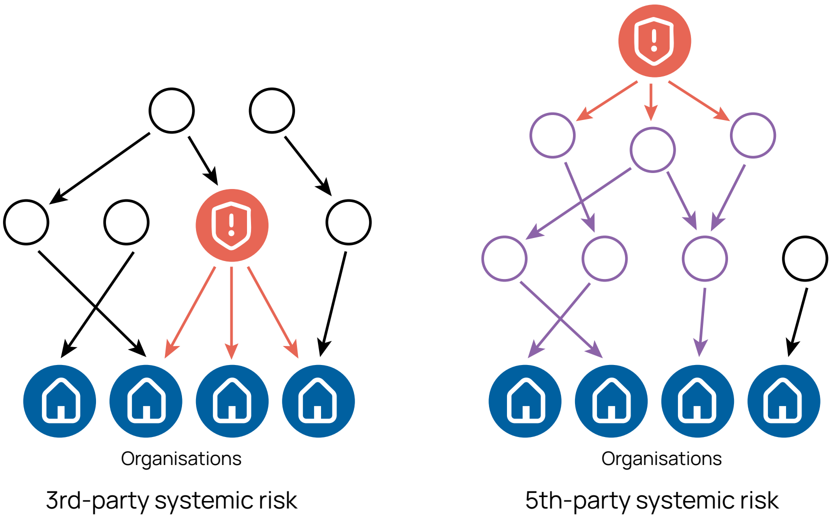


4th-party concentration risk

5th-party concentration risk

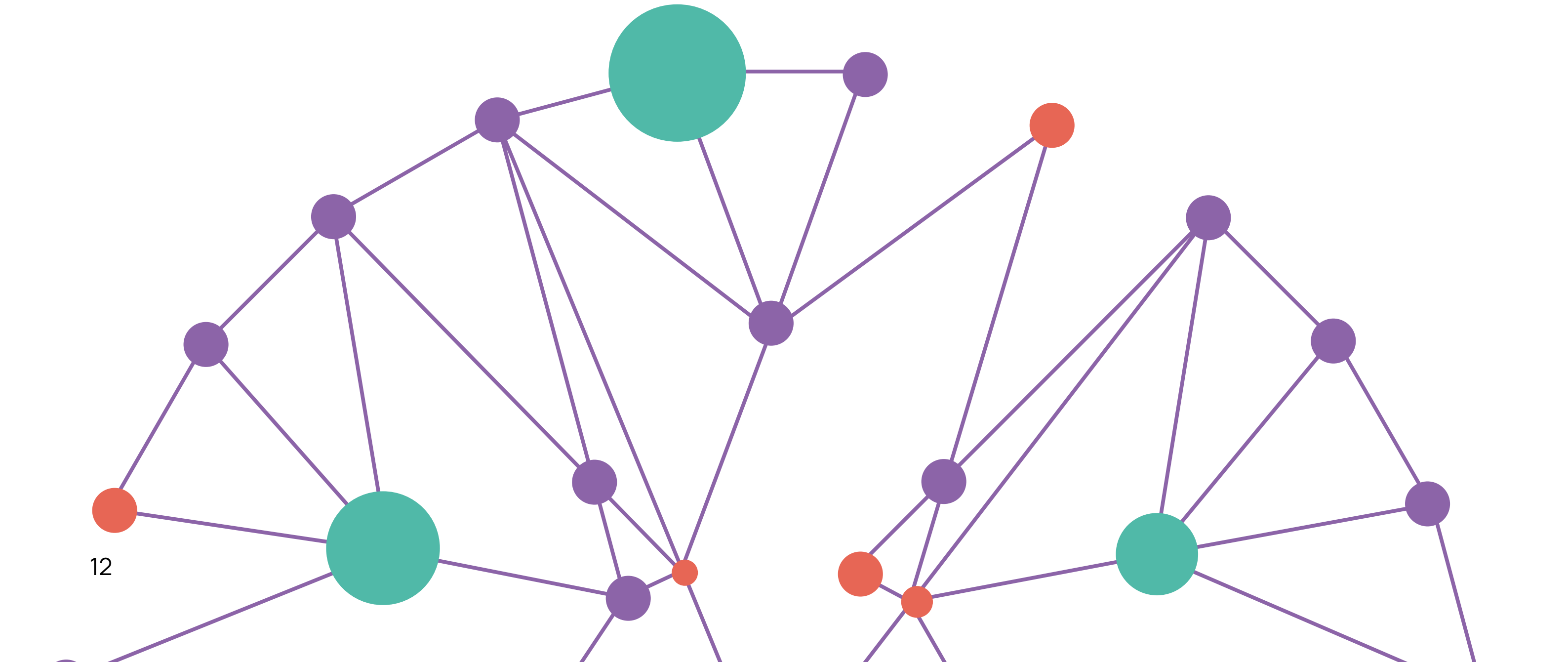
Concentration risks can arise when several critical direct suppliers of an organisation all depend on the same fourth-party (or nth-party) provider for a critical service or function.

Systemic Concentration Risks



Systemic concentration risks are an extension of concentration risks facing individual organisations. They stem from shared suppliers, whose disruption would have a cascading impact across multiple organisations within the same sector.

The new rules and regulations thus put regulated entities into a situation where they must not only manage their own third-party risks, but also contribute to sector-wide efforts to map and understand shared vulnerabilities. This is no small feat. Yet, these regulatory demands have often arrived without proportional support, especially financial support, placing smaller or less well-resourced local authorities under significant strain.



Section 3: Local Authorities Respond to Mounting Cyber Risk & The Enduring Challenges with TPRM

In response to these challenges, and in addition to working towards implementing the LG CAF, one of the most significant sector-led efforts to improve local authorities' collective cyber security posture has been the establishment and strengthening of Warning, Advice and Reporting Points (WARPs). These regional and local operational hubs provide a trusted arena for local authorities to exchange intelligence on emerging threats, vulnerabilities, and incidents in real-time. WARPs have become indispensable in bridging the fragmented nature of local authorities' cyber security efforts, enabling even smaller bodies without dedicated security leadership to benefit from shared knowledge and coordinated action.

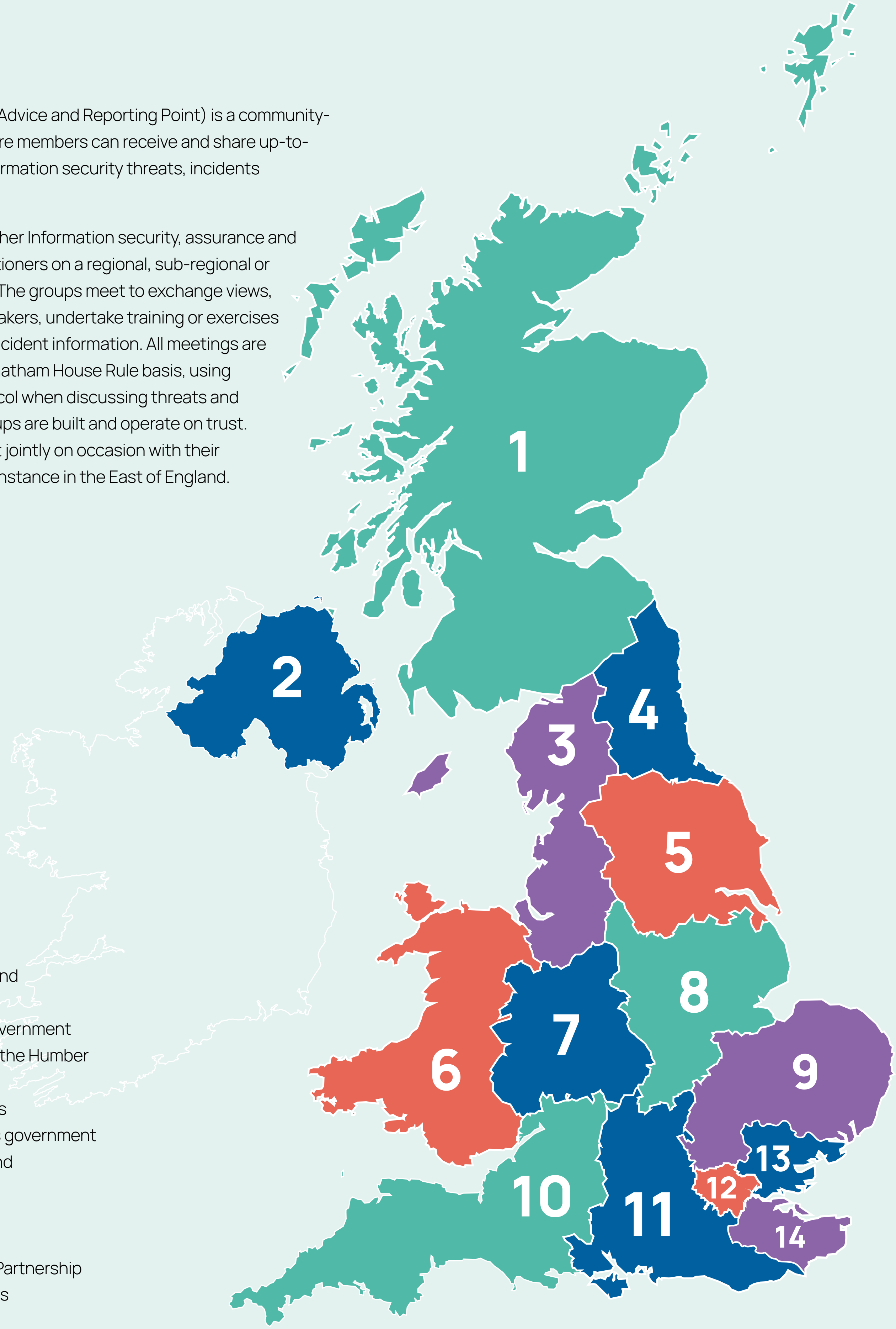
Moreover, local authorities have explored and, in some cases, implemented pooled procurement arrangements for technology and security services, enabling economies of scale that would be unattainable individually. Partnerships with the Local Government Association and other sector bodies have developed training programmes, best practice guidelines, and awareness campaigns tailored to the public sector's unique challenges.

Yet, despite these positive developments and efforts, many local authorities still rely on traditional, manual approaches to managing third-party risks involving spreadsheets, questionnaires, and siloed data collection, which have prevented better supply chain security outcomes.

WARPs

A WARP (Warning, Advice and Reporting Point) is a community-based service where members can receive and share up-to-date advice on information security threats, incidents and solutions.

WARPs bring together Information security, assurance and governance practitioners on a regional, sub-regional or partnership basis. The groups meet to exchange views, listen to guest speakers, undertake training or exercises and to exchange incident information. All meetings are conducted on a Chatham House Rule basis, using a traffic light protocol when discussing threats and incidents. The groups are built and operate on trust. Some WARPs meet jointly on occasion with their Socitm region, for instance in the East of England.



Key

1	Scotland
2	Northern Ireland
3	North West
4	North East government
5	Yorkshire and the Humber
6	Wales
7	West Midlands
8	East Midlands government
9	East of England
10	South West
11	South East
12	London
13	Essex Digital Partnership
14	Kent Connects

The Enduring Challenges of Third-Party Risk Management

The complexity of local authority procurement landscapes presents a formidable challenge for third-party risk management. UK local authorities collectively contract with thousands of suppliers, many of which operate across multiple authorities and other public sector organisations. However, there is no standardised, centralised process for assessing, monitoring, and managing the cyber risks these suppliers might introduce. The resulting picture is one of fragmented, reactive TPRM efforts dominated by inefficiencies.

The operational burden of manually managing supplier risk information is significant, particularly for organisations with limited specialist security staff. Each local authority conducts its own risk assessment activities on the same, shared, vendors, imposing duplicated efforts both on themselves and on suppliers. This inefficiency leads to what industry calls “audit fatigue,” discouraging smaller suppliers from engaging meaningfully with risk management requests.

A further complication lies in the dynamic nature of cyber risk. Supplier profiles and security postures are subject to continuous change, driven by factors such as staff turnover, evolving threat landscapes, and changing tech and software. Static assessments carried out annually or even less frequently can quickly become obsolete, leaving local authorities ill-equipped to respond to incidents or emerging threats in real time. Without mechanisms for continuous supplier monitoring, organisations run a significant risk of having serious blind spots.

Local authorities also experience difficulties enforcing cyber assurance standards for complex, multi-tiered supply chains involving sub-contractors and service providers beyond the immediately contracted supplier. Furthermore, local authorities must balance cyber security investment against other pressing public service priorities.

In summary, TPRM remains a persistent and difficult problem for UK local authorities, compounded by structural, procedural, and resource hurdles. It is clear that relying on isolated, council-by-council approaches is neither sustainable nor sufficient given the scale and urgency of the cyber threat facing local government bodies in the UK.

Growing challenges facing local authorities

Based on 200+ conversations Risk Ledger has already had with local authorities, some of the most common challenges include:

Limited resource

Cyber risks are growing faster than team capacity, meaning local authorities are often operating with limited resources.

Constrained budgets

Rising demand for local authority services and increasing costs have tightened the available budget for cyber security.

Limited response capability

Point-in-time assessments and limited communication channels reduce local authorities' ability to respond effectively to cyber threats.

Inaccurate data

Manual approaches lead to data that is both inaccurate and rapidly outdated, increasing the work needed to maintain reliability.

Low supplier engagement

Suppliers are often discouraged from engaging with TPRM due to the repetitive, manual processes required by each of the 350+ councils.

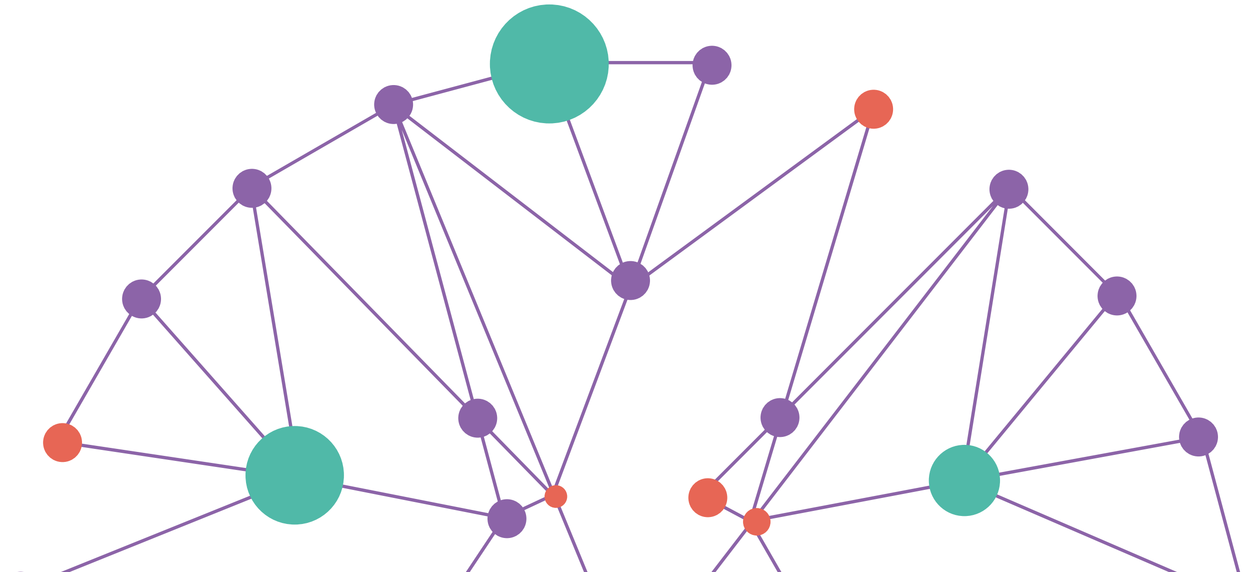
Siloed approach

Processes working in isolation, local authorities can struggle to exert leverage on suppliers and to share critical information effectively.

Section 4: Towards Collaborative Defence: How Local Authorities Transformed Their TPRM

The limitations of fragmented approaches led local authorities and their WARPs to proactively seek new paradigms of collaboration, recognising that a collective defence posture leveraging shared platforms and supply chain intelligence was essential to changing realities on the ground and transforming their supply chain risk management efforts.

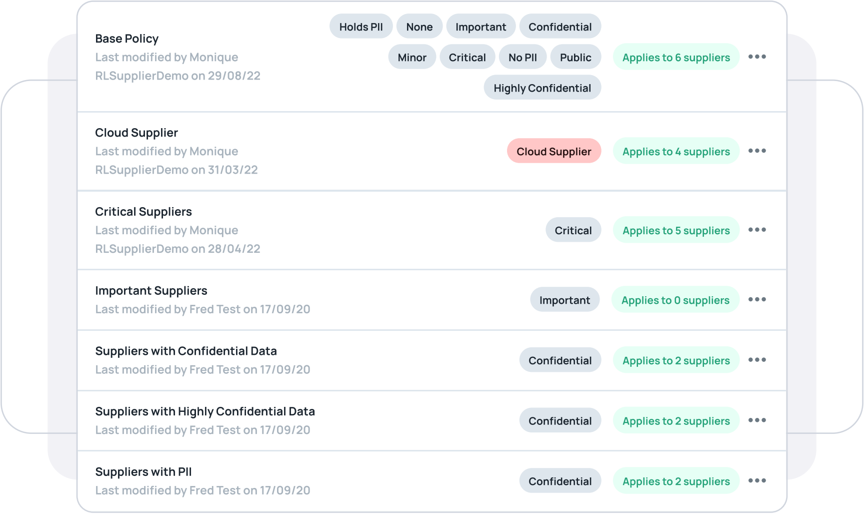
Central to this reimagining of local authorities' TPRM has been the adoption and integration of Risk Ledger, a cloud-based, collaborative supply chain risk management platform designed specifically to address the complexities of third-party risk in public sector supply chains.



How Risk Ledger facilitates enhanced collaboration that generate better TPRM outcomes

Risk Ledger's platform is based on a unique 'social network' approach to supply chain risk management. Similar to a social network, where each supplier organisation has a profile on the platform that contains information about the business, its cyber security controls and other relevant risk areas, including ESG and financial risk. The questionnaires used to generate these profiles are based on Risk Ledger's standardised assessment framework, mapped against leading international standards such as NIST, ISO27001 and the NCSC's CAF.

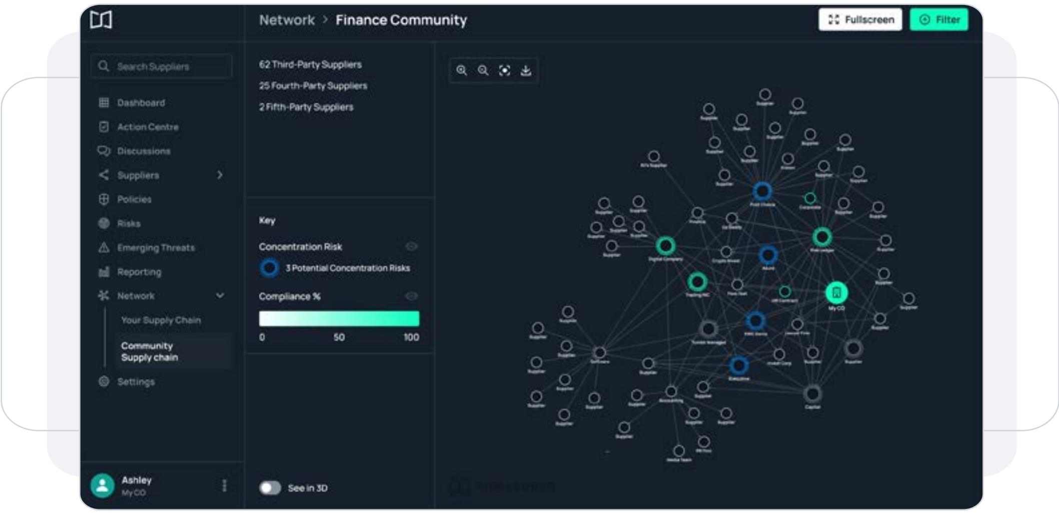
The in-depth supplier profile, controlled by the supplier, is then shared with their connected clients and customers on the platform. This means that suppliers only have to complete, and then keep up-to-date one assessment, significantly reducing assessment fatigue and allowing them to concentrate on what matters most, their own security. Clients can set requirements against the assessment framework, as well as label suppliers based on factors such as their criticality, whether they handle sensitive data, whether they have system access, and more.



Base Policy Last modified by Monique RLSupplierDemo on 29/08/22	Holds PII None Important Confidential Minor Critical No PII Public Highly Confidential	Applies to 6 suppliers	•••
Cloud Supplier Last modified by Monique RLSupplierDemo on 31/03/22	Cloud Supplier	Applies to 4 suppliers	•••
Critical Suppliers Last modified by Monique RLSupplierDemo on 28/04/22	Critical	Applies to 5 suppliers	•••
Important Suppliers Last modified by Fred Test on 17/09/20	Important	Applies to 0 suppliers	•••
Suppliers with Confidential Data Last modified by Fred Test on 17/09/20	Confidential	Applies to 2 suppliers	•••
Suppliers with Highly Confidential Data Last modified by Fred Test on 17/09/20	Confidential	Applies to 2 suppliers	•••
Suppliers with PII Last modified by Fred Test on 17/09/20	Confidential	Applies to 2 suppliers	•••

Importantly, organisations can interact and collaborate directly with the security teams of their suppliers on the platform, on issues such as remediation and risk mitigation. This helps to build strong supplier relationships over time, which support more effective responses to supply chain incidents when they occur and significantly improves supplier engagement.

Since suppliers can also use Risk Ledger to manage their respective supply chain risks by connecting with their own suppliers, thus using Risk Ledger as both a supplier and a client, this uncovers all the hidden connections and middle links in the supply chain and builds a map of interdependencies within wider supply chain ecosystems.

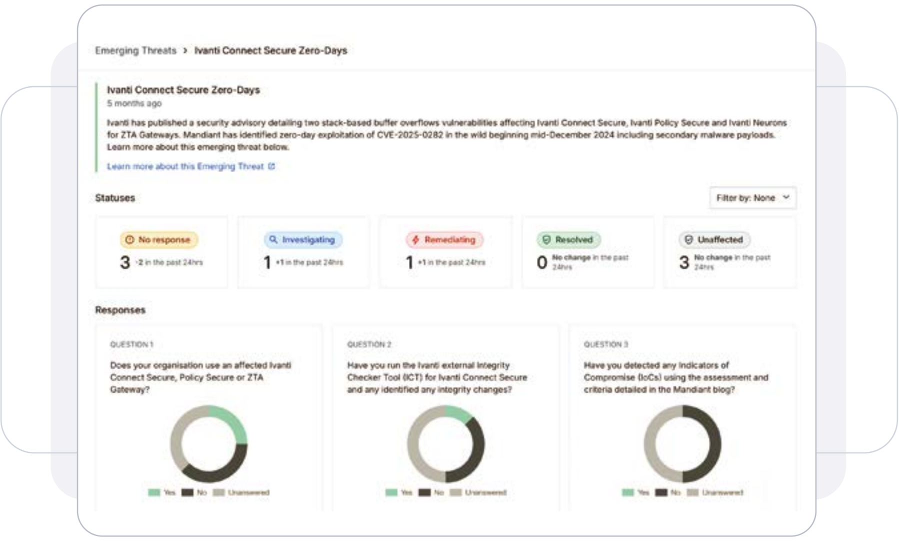


To build on this social network approach, Risk Ledger has also introduced a new community feature that empowers security teams within trusted peer communities to Defend-as-One against supply chain threats. These are composed of organisations that share many of the same problems, or have to comply with the same regulations.

In these communities, members agree to securely share information and supplier risk intelligence with each other, as well as overlay their respective supply chain network maps. This overlaying of organisation's individual maps allows hidden systemic and concentration risks to be uncovered that previously remained hidden. Community members are also encouraged to share best practices, see risks raised against specific suppliers by their peers, mitigate these risks together, and collaboratively lobby unresponsive suppliers.

Moreover, organisations are also able to collaborate on supply chain attacks when they strike, significantly improving their access to up-to-date supplier and other contextual information in order to ascertain how their critical suppliers might be exposed to any attack.

Better incident response during times of crisis



Emerging Threats › Ivanti Connect Secure Zero-Days

Ivanti Connect Secure Zero-Days
5 months ago

Ivanti has published a security advisory detailing two stack-based buffer overflows vulnerabilities affecting Ivanti Connect Secure, Ivanti Policy Secure and Ivanti Neurons for ZTA Gateways. Mandiant has identified zero-day exploitation of CVE-2025-0282 in the wild beginning mid-December 2024 including secondary malware payloads. Learn more about this emerging threat below.

Learn more about this Emerging Threat

Statuses

Filter by: None

No response 3 -2 in the past 24hrs

Investigating 1 +1 in the past 24hrs

Remediating 1 +1 in the past 24hrs

Resolved 0 No change in the past 24hrs

Unaffected 3 No change in the past 24hrs

Responses

QUESTION 1

Does your organisation use an affected Ivanti Connect Secure, Policy Secure or ZTA Gateway?

QUESTION 2

Have you run the Ivanti external Integrity Checker Tool (ICT) for Ivanti Connect Secure and any identified any integrity changes?

QUESTION 3

Have you detected any Indicators of Compromise (IoCs) using the assessment and criteria detailed in the Mandiant blog?

ISfL and SEGWARP Take the Lead

To explore the benefits of this new approach to supply chain security, two WARPs in particular - ISfL and SEGWARP - took the lead and teamed up with Risk Ledger for a project initially including 10 local authorities, and aimed at streamlining their collective TPRM efforts, reduce duplicate workload and harden their resilience to attacks through enhanced collaboration.

Joining together in a dedicated Risk Ledger community for local authorities has provided participants with numerous immediate benefits:

- Access to a network over 12,000 suppliers (and growing) with completed security profiles that have already been vetted by other clients on the platform.
- A much deeper understanding of supplier relationships and dependencies, even beyond their immediate 3rd parties.
- Ability to assess the likely operational impacts of a disruption at a critical ICT 3rd party.
- Visibility into shared risks and their potential impacts.
- Opportunity to collaboratively triage and prioritise risks and develop targeted mitigation strategies.

Enhanced visibility beyond 3rd parties

Immediate access to

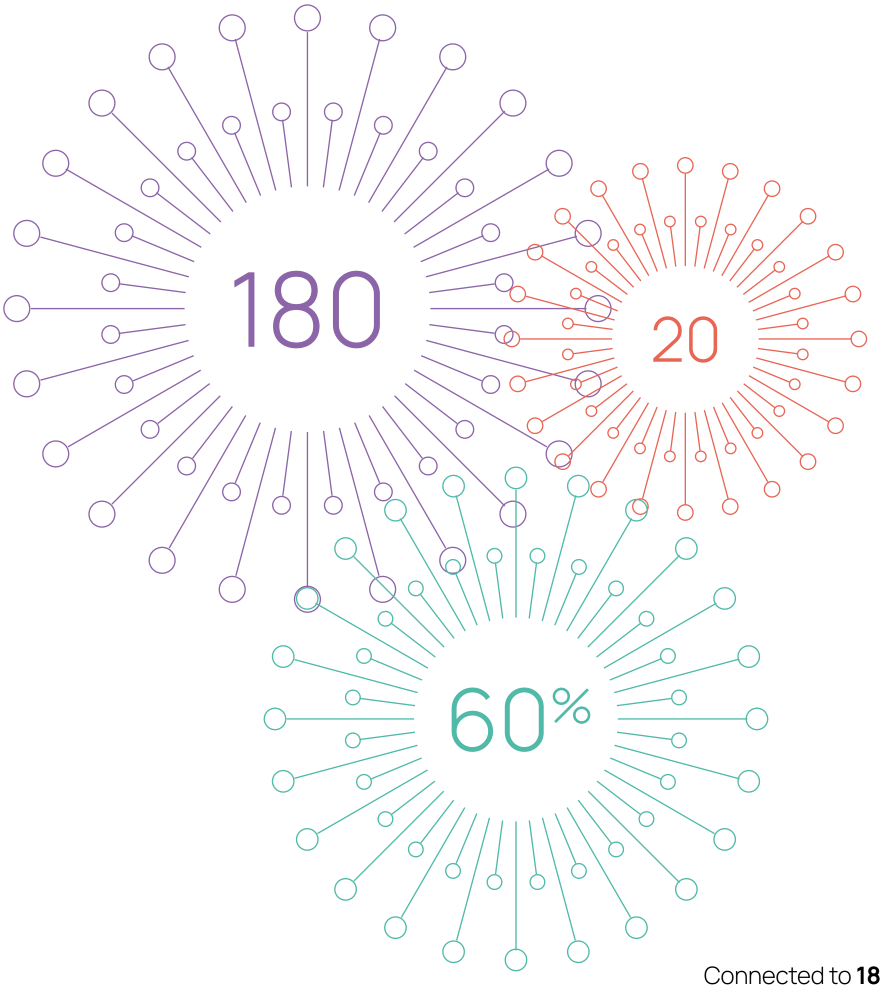
12,000

suppliers and growing

Two Weeks Into the Project

Within a mere 2 weeks after the start of the project, Risk Ledger was able to compare 300 unique supplier names provided by the participants and connect them to 180 of them. This means that local authorities reaped immediate benefits from the fact that **60% of their suppliers** were already using the platform, making the process of connecting with them and reviewing their already completed and peer-vetted security profiles almost instantaneously.

Just by connecting the participants to these 180 direct suppliers and by connecting them into into a community to share their respective supply chain maps, Risk Ledger was also able to identify 20 potential concentration risks that these local authorities were previously unaware of.



Connected to **180** direct suppliers

60% of their suppliers already had completed assessments on Risk Ledger.

20 potential concentration risks identified.

Six Months Into the Project

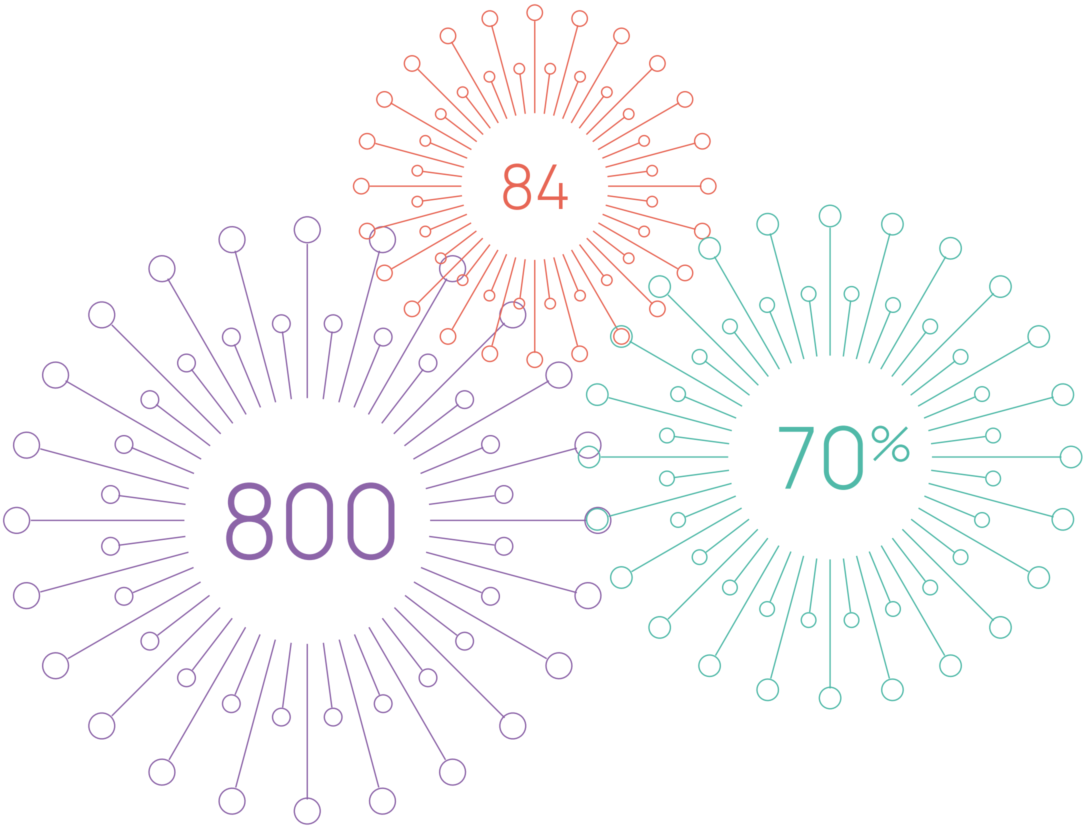
Six months into this unique project, 10 more local authorities and another WARP, South West, have since joined the community and participating local authorities have now connected collectively to an aggregate of 800 plus direct suppliers on the platform. While local authorities joining at the beginning of the project found that on average 60% of all their suppliers were already using the platform, for the more recent participants this number has already increased to 70%.

This growth of the community also allowed the platform to build out a rapidly growing map of the cohort's combined supply chain ecosystem and identify a total of 1048 additional supplier dependencies across these local authorities' n-th parties. Most importantly, this also revealed:

- 84 potential concentration risks
    - Now connected to **800** direct suppliers
    - **70%** of their suppliers already had completed assessments on Risk Ledger
    - **84** potential concentration risks identified

60%->70%

average number of key suppliers already in the Risk Ledger network for new participants.



Out of the 84 potential concentration risks discovered, the analysis further showed:

8

direct third-parties connected to at least 50% of the community members, representing clear potential systemic risks to the community as a whole.

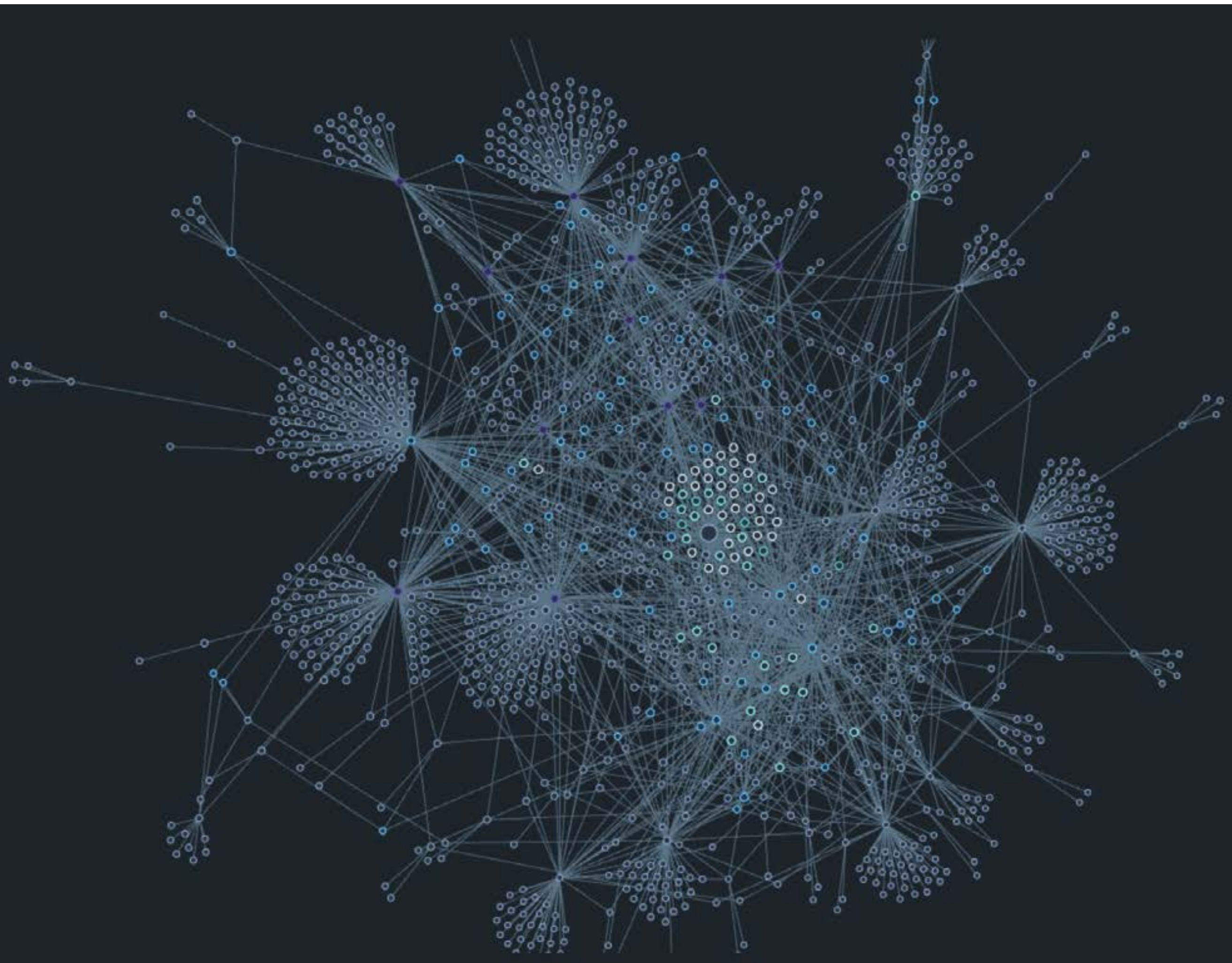
10

fourth-parties connected to 3 or more direct third-parties to local authorities.

1

supplier that is connected to all local authorities, representing a singular, critical point of failure for the entire community and each of its members individually.

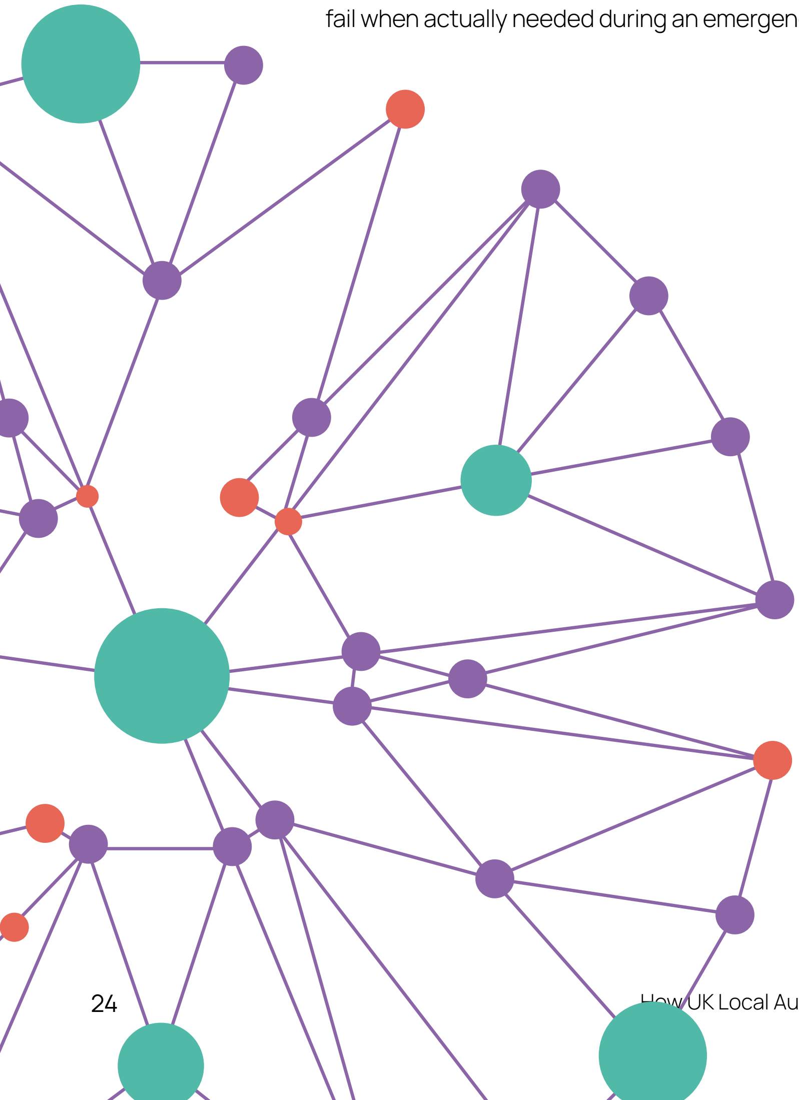
Combined network map of 20 councils after 6 months



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.

Moreover, the data also highlighted further risk factors deserving attention. It revealed, for example, that the adherence to fundamental cyber hygiene measures is inconsistent across local authorities' supplier base. A striking 1 in 4 suppliers serving local authorities do not possess Cyber Essentials certification, for example. This is a material risk, given that the NCSC estimates organisations with this certification are 80% less likely to experience a cyber incident.

Furthermore, other essential technical controls show non-compliance: 10% of suppliers are not conducting regular automated vulnerability scans of their public-facing IT infrastructure, leaving potential vulnerabilities unaddressed. A foundational security failure was also identified, with 4% of suppliers not using Multi-Factor Authentication (MFA) for securing remote access to their network or cloud environments. While suppliers demonstrate a strong awareness of the need for business continuity, the rigour of their preparedness is questionable. An impressive 99% of suppliers report having an approved business continuity plan in place to ensure service continuity in a disaster. However, this paper-based assurance is undermined by the finding that 41% of suppliers do not regularly test or rehearse their Business Continuity and Disaster Recovery plans. This lack of regular testing introduces significant uncertainty, meaning nearly half of the suppliers' plans may fail when actually needed during an emergency.



25%

of suppliers are not Cyber Essential certified

10%

of suppliers are not conducting regular automated vulnerability scans of their public-facing IT infrastructure

4%

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

41%

of suppliers do not regularly test or rehearse their Business Continuity and Disaster Recovery plans

These findings have proven highly valuable to participants, since focussing mitigation efforts on them allows local authorities to quickly plug important security gaps, providing quick and effective security improvements in their supply chains when addressed.

This unprecedented cross-Council collaboration achieved another unique result: Participants can now also drill down and identify systemically critical suppliers among the concentration risks. By confirming which suppliers handle Personally Identifiable Information (PII) or are integrated into critical systems, local authorities can now sharpen their mitigation efforts on the most relevant third parties.

Section 5: Why Collaborative Supply Chain Cyber Defence Works

As discussed earlier, traditional Third-Party Risk Management (TPRM) has fundamental limitations. It is time-consuming, resource-heavy, and often reliant on manually completed supplier questionnaires, making it difficult to identify individual and systemic concentration risks. Additionally, TPRM is typically conducted in silos, preventing organisations from sharing supply chain intelligence and leading to inefficiencies and duplicated efforts.

As the cyber threat landscape grows in sophistication and scale, it is increasingly evident that no single organisation can secure its supply chain in isolation. The highly interconnected nature of today's supply chains means that vulnerabilities within one supplier can rapidly propagate, creating systemic risks that threaten not just individual organisations but entire sectors. Regulators recognise this threat and are now placing greater emphasis on strengthening sectoral resilience, the basis for which is enhanced supply chain visibility, which has thus become a regulatory and strategic imperative for uncovering systemic risks and potential single points of failure that would otherwise remain hidden.

To counter the rising risks posed by supply chain vulnerabilities, industry-wide collaboration between threat intelligence teams has become an established practice. There is close collaboration, for example, between such teams at the largest financial organisations, facilitated by the Financial Services Information Sharing and Analysis Center (FS-ISAC). Similar collaboration exists in other industries. However, the same level of collaboration between peers does not yet exist between third-party risk management (TPRM) teams of different organisations, which continue to work largely in siloes in their own organisations.

Greater collaboration on TPRM, however, can solve many of the traditional challenges with TPRM:

Enhanced Supplier Engagement

A key problem with the state of TPRM is the lack of a commonly accepted standard for assessing the security postures of our suppliers. This is among the leading causes that makes third-party risk management such an arduous and inefficient process, and has prevented greater collaboration. Suppliers commonly receive hundreds of separate questionnaires from their clients all the time, overburdening them and making them spend less time on actually improving their security postures.

By only having to complete one standardised assessment and then being able to share it with all their clients at the click of a button, this significantly reduces the workload for suppliers and allows them to be far more responsive to client requests.

Continuous monitoring

Given that many organisations in the same industry have the same core suppliers, using a standardised assessment framework for supplier due diligence also enables greater burden sharing and thus leads to a reduction in workload and resources needed for local authorities. It also ensures that numerous eyes are on the same supplier at all times, based on the same information - an important step towards taking a more continuous monitoring approach to supply chain risks. It also means that if risks are identified against a specific supplier, this information can be shared with peers and the risks addressed for the benefit of the whole sector, significantly bolstering organisations and entire sectors operational resilience. Through real-time alerts, local authorities now receive instant notifications of changes in any of their suppliers' risk controls and of new incidents or regulatory compliance issues, enabling a dynamic and proactive response rather than a reactive posture reliant on outdated data. Using a standardised assessment framework that is constantly updated to align with new regulations and best practice means individual TPRM teams don't need to keep updating their own frameworks and re-issuing them to suppliers for re-assessment.

Encourage unresponsive suppliers.

Collaborating with peers equally enables organisations to lobby unresponsive suppliers together, increasing the impact of requests and ensuring they are taken seriously.

Enhance supply chain visibility.

Collaborating with peers gives organisations a much better understanding of their own and wider sectoral supply chain dependencies, far beyond third parties. It allows organisations to identify shared systemic risks and better understand the security posture of suppliers beyond direct vendors. It enables organisations to reach out to these more distant connections via peers for whom they may be direct suppliers.

Faster response to emerging threats.

With multiple TPRM teams monitoring the same suppliers, emerging threats or security breaches anywhere in the supply chain can be more quickly identified. Resources can be mobilised more rapidly across the industry to reinforce security or mitigate the risks.

The Power of Collaboration

Combined commercial strength

Collective purchasing power creates genuine incentives for suppliers to invest in their security.

Shared threat intelligence

Real-time insights from across the network, not just your limited view of your suppliers.

Coordinated response

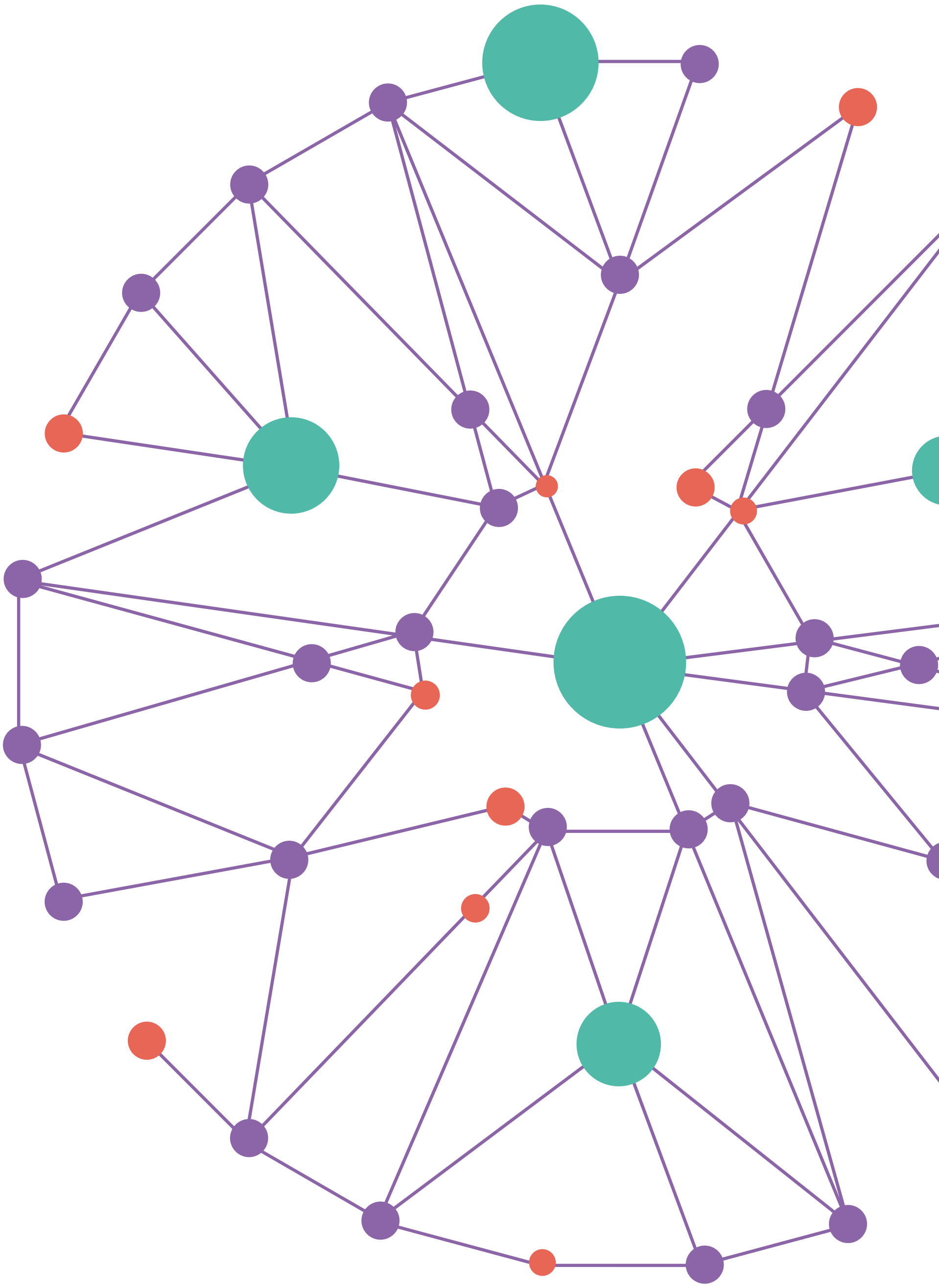
When incidents occur, the entire network responds together rather than organisations scrambling individually.

The local authorities and WARPS that participated in this project realised the opportunity to transform the effectiveness and efficiency of their TPRM programmes and bolster their supply chain security through taking a more collaborative approach.

As participation in the initiative grows, the network effect further amplifies its value. Each new local authoritiy or supplier contributes data that benefits the entire ecosystem, strengthening collective resilience, cumulatively reducing workload and resource demands over time. Local authorities with limited cyber security capability also benefit directly by tapping into expertise and intelligence shared across the sector, thereby levelling up the overall security posture.

By sharing information on their suppliers' security practices and controls, and then collaborating on making the weakest nodes in the system stronger collectively, local authorities can save a lot of time and resources. Even more importantly, it enhances the security of the entire ecosystem.

The longer-term implications are significant. The collaborative model can serve as a blueprint not only for local authorities but also for the wider UK public sector, enabling integrated supply chain cyber risk governance. Integration with national regulatory frameworks and threat intelligence feeds is underway, positioning the local authority sector to influence, and be supported by, broader government cyber strategy.



Conclusion: UK Local Authorities as Pioneers in Collaborative TPRM

UK local authorities have encountered an unprecedented cyber threat environment characterised by rising attacks, abundant vulnerabilities, and severe resource constraints. In response, instead of shying away from this monumental challenge, local authorities, with the support of their WARPS, have decided to tackle the challenge head-on by pivoting from a fragmented, resource-intensive method of managing supply chain cyber risks towards a collaborative, shared defence model championed by technology innovators Risk Ledger.

This transformation embodies a pragmatic and forward-thinking approach—one where local authorities turn inherent limitations into an advantage by pooling intelligence, standardising assurance processes, and leveraging collective scale. By "defending as one," they improve not only their individual resilience but also that of the broader public sector supply chain, and institute a cultural shift away from ineffective, siloed TPRM approaches and towards an active cyber defence discipline.

For policymakers and regulators, the lesson is clear. Supporting this emergent collaborative ecosystem through sustained funding, clear regulatory guidance, and skills development initiatives will be critical to maintaining momentum. The government can play a facilitative role by endorsing shared platforms, incentivising participation, and enabling integration with national cyber threat intelligence operations. Most importantly, they should use this case study of UK local authorities, which clearly demonstrates that necessity is the mother of invention, to make a strong case for collaboration among public sector and indeed private sector bodies operating within the same sectors as an effective new approach to TPRM and supply chain security more generally.

Ultimately, UK local authorities have demonstrated that a proactive, collective approach to third-party risk management is both feasible and effective.
By championing this new paradigm, they not only protect vital services and citizen data today but establish a scalable model that can strengthen public sector cybersecurity into the future.

> “Risk Ledger has removed our dependency on spreadsheets and admin work. It allows us to create a request and easily automates the workflow, allowing our team to complete other crucial activities and saving hours of time. It has also created value for our suppliers leading to less pushback than we have come to expect.”

City of Westminster

> “Using Risk Ledger to centralise our third-party risk process is helping Wokingham gain visibility on systems and suppliers that have previously been missed, which is helping reduce risk in the council.”

WOKINGHAM
BOROUGH COUNCIL

RISK LEDGER

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

Company registration number (England & Wales): 10831970

Contact: www.riskledger.com I marketing@riskledger.com I +44 1234 567890