RISK LEDGER

Identifying Concentration Risks in Financial Services Supply Chains

Foreword

Cyber security once seemed akin to medieval warfare – organisations built walls and moats in the form of firewalls and intrusion detection systems to protect their most critical assets. However, as businesses have moved to cloud-based services and relied on critical third parties to provide Information and Communication Technology (ICT), the traditional perimeter defence model became obsolete.

Today, financial institutions operate within a complex web of interdependencies that could extend beyond third-party, into fourth-, fifth- or nth-party suppliers – sometimes including other financial institutions. This has widened the attack surface beyond their immediate visibility.

Regulators are acutely aware of the risks that supply chain attacks can pose to many critical sectors, especially finance. As a result, they have introduced regulations like the Digital Operational Resilience Act (DORA) to increase visibility into supply chain dependencies and mitigate systemic risks to the financial sector.

However, compliance with regulations is not enough. We believe that collaboration is the most effective way to stay ahead of these threats. This project demonstrates how financial institutions can work together to address third-party risk management challenges – such as inefficiencies and lack of supplier engagement – and uncover hidden supply chain risks, which a single institution could not do alone.

Acknowledgements

We would like to thank Dr David Aubrey-Jones, Third Party Risk Lead at the Financial Services Information Sharing and Analysis Centre (FS-ISAC), for his collaboration on this project. Together, we share the belief that addressing systemic concentration risks in the financial sector requires greater collaboration both between organisations and across internal teams. His insight and perspective helped shape the direction of this project and supported the broader goal of improving supply chain visibility and resilience across the industry.

Contents

Executive Summary

The strategic challenge of cyber and resilience risks in the supply chain

Supply chain cyber incidents are increasing in both frequency and impact, often originating from suppliers within an organisation's extended supply chain. Financial institutions face a critical challenge – they lack the tools to map and analyse their supply chains efficiently, leaving them vulnerable despite new regulatory requirements to identify concentration risks. These risks stem from the growing number and complexity of dependencies that exist in current supply chain relationships and outsourcing arrangements.

Given the financial sector's shared reliance on numerous critical suppliers, these risks are not just relevant to individual financial institutions, but represent a broader risk to the security and resilience of the sector as a whole.

Our approach

Risk Ledger collaborated with Dr David Aubrey-Jones of FS-ISAC to design and execute this pilot project to demonstrate the power of collective intelligence in identifying individual and systemic concentration risks.

For this effort, we agreed to limit the cohort to six financial institutions to provide a meaningful participant pool likely to uncover systemic concentration risks.

Using Risk Ledger, a third-party risk management platform, participants connected with their critical third parties, gained visibility into their extended supply chains, and identified previously unknown risks.

The first phase of the project involved mapping out the extended supply chains for each participant. Participants provided a list of their critical third parties that was imported into Risk Ledger, which then displayed the connections amongst their third-, fourth-, fifth-, and nth-party suppliers.

The second phase involved placing the six participants into a dedicated Community on Risk Ledger – an isolated, secure environment where their respective supply chain data was made visible to one another. This collective view enabled a comprehensive mapping of the cohort's extended supply chain, revealing systemic concentration risks that traditional and siloed third-party risk management (TPRM) approaches would fail to uncover.

Key Findings

Supplier dependencies

The cohort provided a combined list of 395 third-party suppliers. When analysed through Risk Ledger, this uncovered a supplier ecosystem extending to as far as seventh parties:

395 Third-Party Suppliers

326 Fourth-Party Suppliers

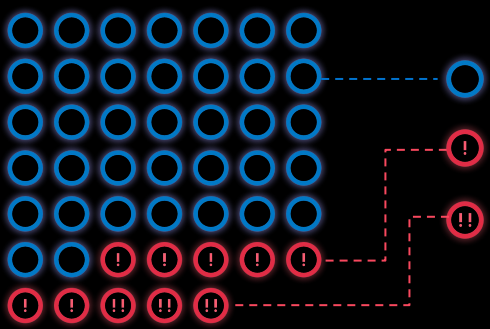
236 Fifth-Party Suppliers

270 Sixth-Party Suppliers

45 Seventh-Party Suppliers

Systemic concentration risks

Risk Ledger identified the following systemic concentration risks across the cohort:



47 systemic concentration risks

38 suppliers were identified among fourth parties and beyond.

9 suppliers were identified as critical third parties, each directly connected to at least 50% of the participants.

3 of the 9 third-party concentration risks were smaller suppliers that participants were unlikely to know they shared.

NOTE: *References to concentration risks in this report indicate potential risks. It is for each institution to assess whether a supplier poses a material risk in their specific context.*

The findings reveal the scale and complexity of supply chain risk in the financial services sector. Despite involving just six participants, the analysis uncovered almost 1,300 supplier dependencies, highlighting the high level of interconnectedness. It also identified 47 systemic concentration risks, a number far greater than the size of the group, which could only be detected through collaborative analysis rather than individual efforts.

Nine third-party suppliers were directly connected to at least half of the participants, while three of the nine were smaller suppliers whose importance to the cohort as a whole would have likely gone unnoticed. This points to a broader sector-wide reliance on a small group of providers, with individual firms often unaware of these shared critical dependencies. The findings make it clear that systemic risks cannot be identified in isolation. **A collaborative approach is essential to uncover shared risks and strengthen the overall resilience of the financial sector.**

Recommendations

Leverage the power of TPRM programmes

- Improve collaboration between Threat Intelligence, Operational Resilience and TPRM teams.
- Improve supplier relationships to expand supply chain visibility.
- Enable continuous monitoring to track changes in suppliers' security postures.

Defend-as-One with your peers

- Uncover hidden risks through collaboration.
- Share risk insights and supply chain intelligence amongst trusted peers.
- Move beyond compliance. Proactive collaboration – not just regulation – is critical to operational resilience.

Address roadblocks to greater information sharing

- Regulators and financial institutions should engage in a dialogue to explore and address any legal uncertainties regarding sharing supply chain information between institutions.
- Regulators could facilitate enhanced collaboration and empower financial entities to proactively uncover and address systemic risks to their industry.

Next steps

Given the success of this project and lessons learned, Risk Ledger will commit to the following actions:

- Explore the feasibility of an expanded project with more financial institutions.
- Engage with industry organisations to demonstrate the power of collaboration in addressing the cyber security and resilience challenges facing financial sector supply chains.
- Develop product enhancements to address the challenges identified during this project.

Conclusion

This project demonstrated that comprehensive supply chain visibility and the identification of concentration risks can be achieved through a Defend-as-One approach. Only through collaboration and shared intelligence can the industry proactively uncover and mitigate hidden dependencies before they escalate into significant risks to the sector.

Overview

Overview

Supply chain cyber attacks and outages are becoming more frequent and impactful, resulting in widespread disruption and affecting entities from individual institutions to entire sectors. While some incidents targeted well-known organisations, others have compromised lesser-known – but nonetheless critical – suppliers to the sector, demonstrating how hidden dependencies can trigger cascading effects.

As supply chains become increasingly interconnected, attackers will continue to exploit this threat vector. Supply chain attacks are seen as appealing, given that a breach at a single supplier may result in many victims, or be leveraged as an avenue to breach a well-defended target. Similarly, an outage or interruption at one provider may impact a multitude of financial institutions. The ability of an organisation to remain secure and resilient depends as much on the security of the entire supply chain as it does on their own defences.

The European Union Agency for Cyber Security (ENISA) predicts that by 2030, supply chain compromise of software dependencies will become the leading cyber threat. This direction of travel underscores the need for a holistic, collaborative approach to supply chain cyber security more generally, strengthening the operational resilience and security of not just individual organisations, but across the sectors in which they operate.

New and emerging regulations recognise the potential sector-wide impact of supply chain incidents. These regulations target the risks related to critical third-party Information and Communications Technology (ICT) suppliers across a variety of sectors including: the financial sector, public sector, and critical national infrastructure. In the EU, these include the Digital Operational Resilience Act (DORA) and Network and Information Security Directive 2 (NIS2). In the UK, operational resilience rules such as Operational Resilience: Critical Third Parties to the UK Financial Sector (PS16/24 and SS6/24), introduced by the Bank of England, Financial Conduct Authority (FCA) and the Prudential Regulation Authority (PRA), aim to strengthen the financial system's resilience through enhanced measures across a variety of areas. This includes governance, risk management, and incident reporting.

A key focus of these regulations is to increase transparency into supplier dependencies across a financial entity's supply chain. For example, DORA requires financial entities to disclose detailed information on product and service-level agreements, supplier criticality, and the extent of their suppliers' reliance on subcontractors and other downstream dependencies. This is to gain a much clearer view of the financial sector's supply chain dependencies to identify systemic risks that could undermine the operational resilience of the entire sector.

Challenge: TPRM is Broken

Financial institutions are increasingly required to identify cyber security risks emanating from their dependence on external suppliers and service providers, yet traditional TPRM programmes struggle to detect often hidden concentration risks in today's complex supply chains. The key issues with traditional TPRM are:

Lack of visibility beyond third parties

- Most organisations only have visibility into their third parties, and lack an understanding of the dependencies and concentration risks that exist at fourth parties and beyond. For example, a primary and backup third-party supplier might rely on the same fourth party. Incident response plans that rely on the availability of the backup supplier may fail if the fourth-party supplier experiences an incident.

- While some organisations have contracts requiring third parties to disclose their subcontractors, this is not uniform across all supplier relationships, let alone across the entire financial sector.

Siloed approach to risk management

- Operational Resilience, Threat Intelligence, and TPRM teams often operate in silos, limiting an organisation's ability to gain a holistic view of supply chain risks.

- While they may leverage similar supplier data, the focus, and outcomes of these teams are typically distinct.

- Additionally, this siloed approach applies to external collaboration, as TPRM teams lack consistent coordination with their counterparts at peer institutions.

Lack of comprehensive intelligence to identify and respond to unknown risks

- Organisations may struggle to respond quickly to emerging supply chain threats without the ability to understand which suppliers are at risk.

- Most organisations do not monitor their entire supply chain for risk signals, or share intelligence with their suppliers.

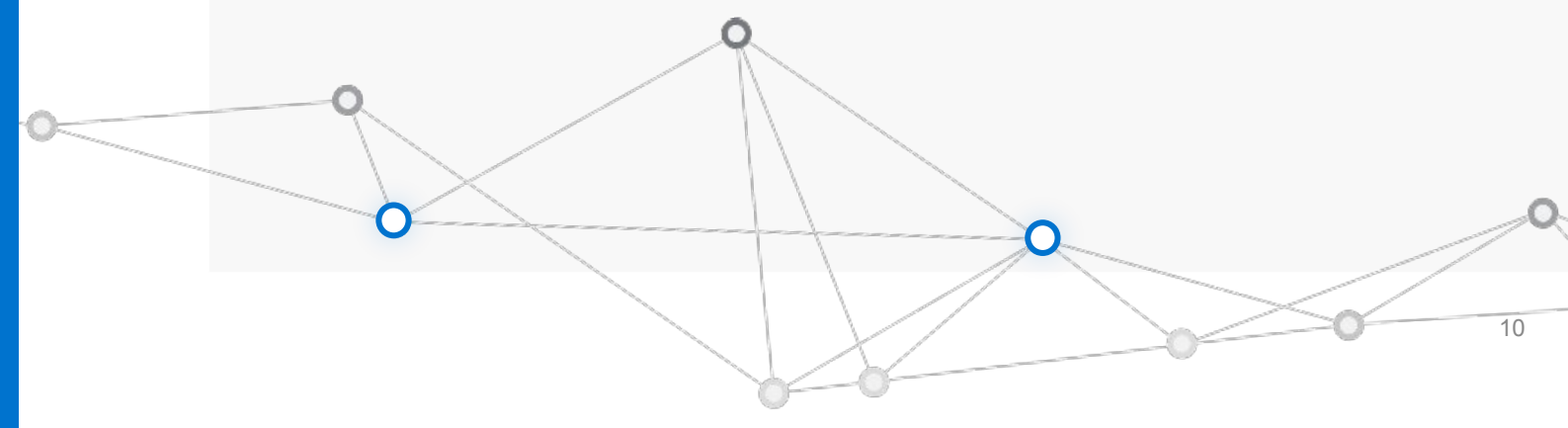
These legacy issues undermine the effectiveness of current TPRM programmes, leaving them inadequate to address the current operational and threat landscape.

Project Objectives

This project aimed to demonstrate how a collaborative approach to third-party risk management can address critical gaps in supply chain visibility facing financial institutions. By using Risk Ledger, participants gained a comprehensive view of their extended supply chain, proving how collaboration can enhance operational resilience by proactively uncovering risks.

The four main objectives:

1. **Objective 1:** Facilitate connections between participants and their suppliers on Risk Ledger, enabling participants to view granular, accurate, and up-to-date information on the security and resilience maturity of their suppliers.
2. **Objective 2:** Map the extended supply chains of participants and assist them in identifying dependencies at fourth-, fifth-, and nth-parties.
3. **Objective 3:** Identify individual concentration risks within each participant's supply chain.
4. **Objective 4:** Identify shared systemic concentration risks across the cohort and demonstrate the efficiencies and benefits of collaboration, through the sharing of best practices, insights, and risk signals.



Digital Operational Resilience Act

The EU Digital Operational Resilience Act includes a new aspect in the regulation of financial services: specific regulation for critical third-party service suppliers. Driving this is a major concern about third-party concentration risk and how this might result in a systemic impact to financial services.

Articles 31-44 titled Oversight Framework of Critical ICT Third-Party Service Providers addresses this concern. The three European Supervisory Authorities (ESA) are required to assess and designate the ICT third-party suppliers deemed critical using criteria specified in Article 31. The ESAs will use 11 quantitative and qualitative indicators, along with the necessary information to build up and interpret such indicators, following a two-step approach. The European Banking Authority (EBA) recently announced the timelines for the designation of critical third-party service suppliers, leveraging the third-party registers of information that financial institutions are required to complete. Critically, assessments will be completed by the end of July 2025, with a hearing period in September and final designation and engagement by the end of the year.

DORA also contains specific requirements for financial institutions to assess and mitigate concentration risk. While resilience and security checks are now generally part of TPRM, DORA significantly raises the bar. Article 28.4c requires firms to "identify and assess all relevant risks in relation to the contractual arrangement, including the possibility that such contractual arrangements may contribute to reinforcing ICT concentration risk as referred to in Article 29."

Article 29 covers the Preliminary Assessment of ICT Concentration Risk at Entity Level. There are several requirements for financial entities when contracting third-party services supporting critical or important functions. Firms must "take into account" if their contractual arrangements would result in:

- Contracting a third-party provider that is not easily substitutable; or
- Multiple contracts with the same ICT third-party service provider or with closely connected ICT third-party service providers.

In such cases, firms need to weigh the benefits and risks of alternative solutions, such as using another provider.

Financial institutions also need to weigh the benefits and risks that may arise from subcontracting, in particular for subcontractors in a third country. This includes compliance with EU data protection rules and the enforcement of the law in that third country. Institutions need to assess whether potentially long or complex chains of subcontracting may impact their ability to fully monitor the contracted functions (article 29.2).

Understanding Concentration Risks

Criteria for classifying concentration risks

A supplier was classified as a concentration risk if it was connected to at least three or more entities within a participant's supply chain. It was considered a systemic concentration risk if it was connected to three or more entities within the cohort's combined supply chain.

Given the limited number of participants in this project, the threshold of three connections was chosen to balance between identifying meaningful concentration risks while avoiding excessive noise. This threshold is adjustable and can be tailored based on contextual factors, risk tolerance, or evolving requirements.

Individual concentration risks

Individual concentration risks arise when a financial institution holds multiple contracts with the same supplier, or when several suppliers within its supply chain depend on a common supplier. As illustrated in Figure 1, this type of risk is represented by a fourth-party supplier supporting three distinct third-party suppliers.

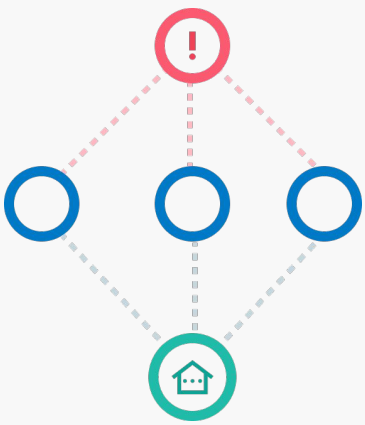


Figure 1: Individual concentration risks

Systemic concentration risks

Systemic concentration risks are an extension of individual concentration risks. While individual concentration risks arise from suppliers whose disruption would impact a single financial institution, systemic concentration risks stem from suppliers whose disruption would have a cascading impact across multiple organisations. Figure 2 shows the downstream impacts of a fourth-party systemic concentration risk.

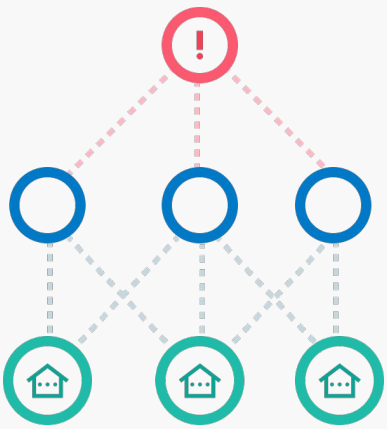


Figure 2: Systemic concentration risks

Key Findings

Key Findings

Each participant provided a list of their critical third parties, resulting in a total of 395 distinct suppliers. After mapping each participant's extended supply chain, the entire cohort was placed into a closed community on Risk Ledger, allowing participants to securely view each other's supply chain data. This collective view enabled a comprehensive mapping of the cohort's extended supply chain, revealing not only its size and interconnectedness, but also previously unknown systemic concentration risks.

Network size

Based on the 395 third-party suppliers initially provided by the participants, the project uncovered an additional 877 suppliers present at fourth parties and beyond, resulting in a grand total of 1,272 suppliers. This mapping extended as far as the seventh party.

- 326 Fourth-Party suppliers
- 236 Fifth-Party suppliers
- 270 Sixth-Party suppliers
- 45 Seventh-Party suppliers

Systemic concentration risks

47 systemic concentration risks were identified among the 1,272 suppliers. As described earlier, systemic risks were defined as suppliers with three or more connections across the cohort map – a threshold chosen for this project to balance the identification of meaningful risks with the need to minimise excessive noise.

- **38 systemic concentration risks** were identified among fourth parties and beyond.
- **9 third-party suppliers** were used by at least 50% of the participants.
- **3 of these 9 third-party suppliers** were smaller suppliers that would have otherwise gone unnoticed.

Summary of Findings

These findings highlight the scale and complexity of the challenge facing the financial services industry.

First, the interconnectedness of supply chains was clearly demonstrated: despite a relatively small group of six participants, Risk Ledger mapped nearly 1,300 suppliers across their extended supply chains.

Second, while 47 systemic concentration risks may appear modest relative to the total number of suppliers, they represent a nearly eightfold multiple compared to the size of the cohort. More importantly, none of these risks would have been visible to any one institution acting alone; they were only identified through a collaborative approach.

Third, the discovery of nine third-party suppliers directly connected to at least half of the participants, including three smaller suppliers, illustrates a broader concern: the sector-wide reliance on a limited number of suppliers. This level of dependency highlights how critical third-party relationships can quietly evolve into systemic concentration risks – risks that are not visible when viewed solely through the lens of an individual organisation's TPRM and resilience planning efforts.

Collectively, these findings 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 a more informed and resilient financial sector.

Network Map

Figure 3 illustrates the cohort's extended supply chain map, generated from the cohort's shared Community space on Risk Ledger. The map displays 1,272 suppliers as white circles, with participants represented as green circles and the 47 systemic concentration risks shown as blue circles.

Figure 3: Cohort network map

Risks of Supply Chain Dependencies

Depending on participants' relationships with their suppliers, and the suppliers' position in the supply chain, there are several ways that participants could be impacted if suppliers were to experience an incident:

- **Disruption of critical services.** Financial institutions and their critical third parties may rely on suppliers that support critical or important functions. Any disruption at these suppliers – cyber or otherwise – may significantly impact an institution's operations.
- **Experiencing a material cyber incident.** Compromised suppliers could serve as an attack vector for malicious actors. Threat actors may exploit the nature of their business relationship (e.g., software or managed services) to breach participants' systems. Confidential data could be stolen or its integrity compromised. Additionally, malicious actors could use the connections in these participants' supply chains to target additional victims.

While well-known, heavily relied-upon third-party suppliers (e.g. leading cloud suppliers, clearing houses, messaging services) could typically be considered as systemic concentration risks, this project drew attention to the fact that systemic concentration risks can also stem from smaller – yet not necessarily less impactful – suppliers. This analysis identified three such suppliers in particular that the cohort would have unlikely been aware they shared.

To be clear, the categorisation of these suppliers as systemic concentration risks is not based on any negative observation of their maturity in managing cyber risk. Rather, it is a recognition that as a market leader in their respective service offerings, they have a significant number of clients in the financial services sector.

It is likely that many additional financial institutions also rely on these same suppliers. Therefore, an incident at any of these would likely result in a significant impact across the entire sector. Understanding and mitigating this impact is one of the key goals of DORA and UK PS16/24 Critical Third Parties to the UK Financial Sector.

While identifying a concentration risk can highlight potential exposure, it does not necessarily warrant switching to an alternative supplier. Rather, it should guide decision-making and inform a re-evaluation of the supplier's risk profile in the context of this new information. By weighing the supplier's potential benefits (e.g. cost efficiency, security maturity, redundancy capability) against identified risks, organisations can consider whether additional controls are needed to maintain alignment with senior leadership's risk appetite.

Challenges

Challenges

Several key challenges emerged that hindered the efficiency and effectiveness of this project. These included internal silos between participants' key teams, institutional hesitancy in sharing supplier data, and limited supplier engagement. Addressing these will be important for improving any potential future iterations of this project.

Lack of collaboration between internal teams

Many participants' Operational Resilience and Threat Intelligence teams had little to no engagement with their TPRM teams, despite their shared interest in understanding supply chain risks. Since TPRM teams hold supplier lists and key contextual data, their involvement was essential, but often delayed. One participant noted that this project was the first time their teams had worked together. These internal silos slowed progress and caused staggered participant onboarding, delaying the ability to identify systemic concentration risks collectively.

Internal barriers to sharing supplier lists

Policies restricting data sharing made it difficult for participants to provide supplier lists quickly, delaying their ability to use Risk Ledger to establish connections with their suppliers. While many Threat Intelligence teams share information via other channels, TPRM teams typically do not operate in this way.

Additionally, participants required Risk Ledger to undergo an extensive due diligence and supplier onboarding process, despite this project being structured as a proof of concept. Overcoming these internal roadblocks requires a cultural shift toward secure, industry-wide intelligence sharing, a shift that regulators may be able to facilitate.

Limited supplier engagement

Participants who were not already clients of Risk Ledger faced challenges in identifying individual concentration risks due to limited visibility into nth-party suppliers. This was largely the result of the project's short timeframe, which limited their ability to onboard their critical suppliers. This is an essential first step to iteratively map the extended supply chain. In contrast, participants who were existing Risk Ledger clients benefited from previous supplier engagement, where their supply chains were already in place.

Recommendations

Recommendations

Risk Ledger successfully identified systemic concentration risks that, when viewed through the lens of a single institution, may not have been previously identified as a concentration risk. Expanding the size of the financial services community on Risk Ledger would allow institutions to uncover hidden systemic concentration risks more quickly, as well as identify additional systemic concentration risks impacting the sector. This would aid regulators, in safeguarding the stability of the financial sector.

Uncovering these risks is crucial for providing senior leaders with a comprehensive understanding of the operating landscape and enabling well-informed decision-making. Without insights into these unrecognised risks, leaders cannot fully account for them in strategic and tactical planning, resulting in decisions and initiatives that are less robust than intended.

Identifying these risks is only the first step. To begin developing an effective strategy towards addressing them, financial institutions need to:

- Improve collaboration within internal teams to enhance current TPRM processes by ensuring all teams have the contextual information necessary for security and operational resilience planning.

- Collaborate with peers and leverage their shared expertise by exchanging supplier data, risk intelligence, and mitigation strategies to increase efficiencies.

- Adopt proactive risk management rather than waiting for regulators' conclusions or insights.

DORA and similar operational resilience regulations hope to address supply chain risks by requiring enhanced controls regarding continuous monitoring, incident reporting, and contractual requirements. Additionally, they require financial institutions to gain detailed visibility not only into their suppliers, but into the contextual relationship between the suppliers: the business functions that rely on these services as well as their criticality of those functions. With this information, the regulators aim to understand and help mitigate the systemic risks facing the financial sector. As this project demonstrated, collectively mapping supply chains and sharing intelligence allows financial institutions to proactively identify and respond to systemic risks.

A mature third-party risk management approach recognises that visibility, collaboration, and a proactive approach are key to enhancing security and resilience. Financial institutions must move beyond basic regulatory compliance and work together to build a more robust security and operational resilience strategy.

Based on the findings of this project, we recommend the following:

Recommendation 1:
Defend-as-One with your peers

Systemic concentration risks can only be effectively identified through a comprehensive analysis of the extended supply chains across a sector. This project demonstrated how creating a secure, shared environment for participants to view each other's supply chain data enabled the identification of systemic concentration risks across the cohort.

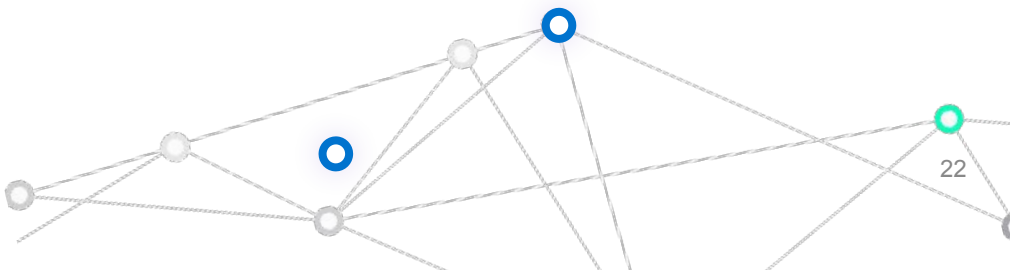
Only by enhancing collaboration and sharing of granular data (e.g. suppliers, control assessments, criticality ratings) can financial institutions understand the full impact of a disruption to a critical third party. By working together, organisations can triage risks more effectively, prioritise systemic risks, and develop shared mitigation strategies.

Actions to consider:

- Expanding the financial services community on Risk Ledger increases the number of trusted institutions contributing to systemic risk identification. Greater participation enhances visibility into shared risks, enabling stronger collective mitigation strategies and improved sector-wide operational resilience.

- Share details of supplier relationships to differentiate between shared suppliers and actual concentration risks. Not all shared suppliers pose systemic risks; legitimate risks are those where a disruption would impact critical functions across multiple organisations. Information sharing can be structured to identify concentration risks while maintaining the confidentiality of sensitive business information that institutions may be unwilling to share with competitors.

- Adopt collaborative TPRM. Sharing risk assessments and signals related to supplier security posture among trusted peers enables institutions to collectively engage with suppliers. This collective approach may be more effective in encouraging suppliers to address risks, compared to individual institutions acting alone.



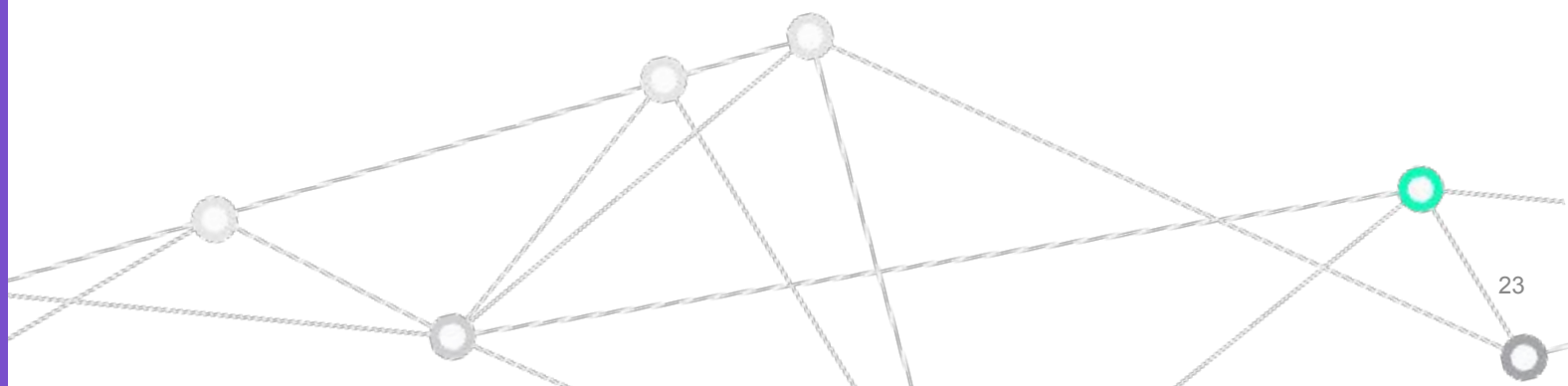
Recommendation 2:
Leverage the power of TPRM programmes

The financial sector generally has more mature TPRM programmes than other industries. Occasionally, this maturity results in a reluctance to adapt and improve TPRM in response to evolving threats or opportunities. Importantly, developing the capability to identify concentration risks does not require the development of an entirely new programme.

By incorporating tools like Risk Ledger, already used by many organisations to assess their suppliers' security, organisations can begin to map the middle links to reveal wider network dependencies. This approach enables organisations to leverage the granular data already collected by their TPRM teams, and turn it into actionable intelligence on concentration risk exposure.

Actions to consider:

- Encourage suppliers to share visibility into their own supply chains. Platforms like Risk Ledger allow suppliers to connect with their own critical suppliers, helping establish the middle links in the supply chain.
- Develop contractual clauses for suppliers to share supply chain information. As DORA and other regulations bring critical third parties into scope, suppliers have an added incentive to disclose their own dependencies.
- Establish internal supply chain risk working groups to align TPRM, Operational Resilience, Cyber Security, Compliance, and Threat Intelligence teams. Fostering a more collaborative environment ensures that supplier data is used effectively to identify concentration risks while managing concerns about sensitive business operations.

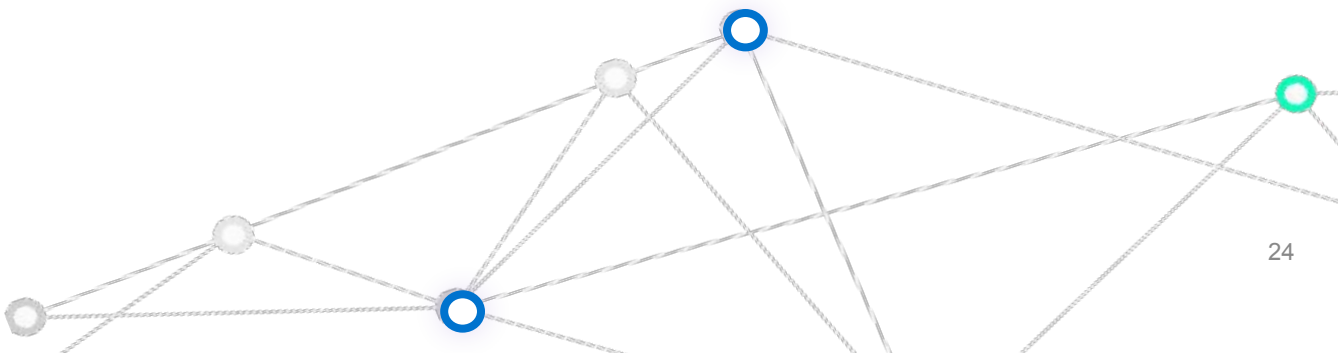


Recommendation 3:
Address roadblocks to greater information sharing

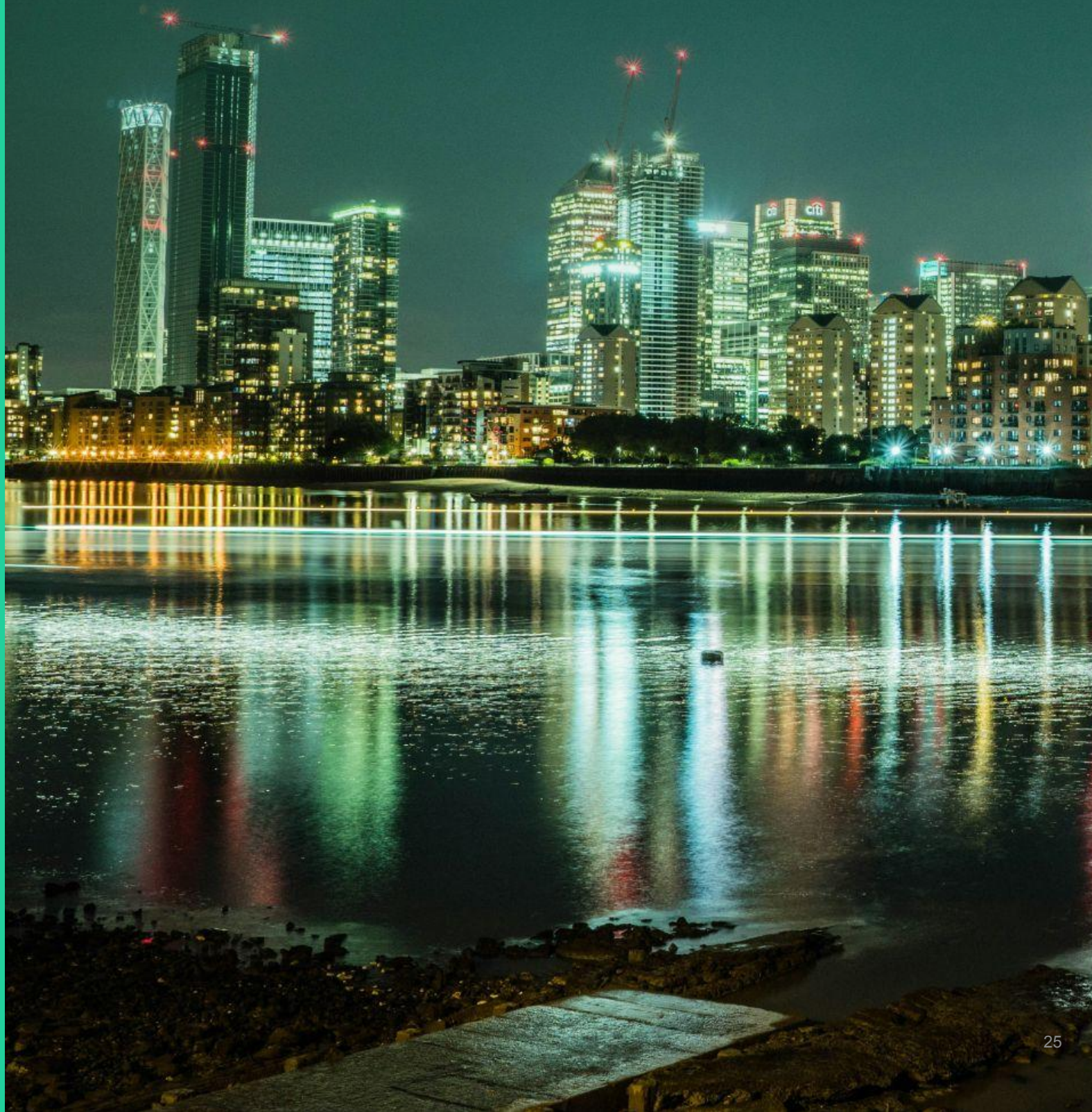
DORA is a step in the right direction for enhancing the resilience of the financial sector. However, this project has underscored the critical role of collaboration in identifying systemic risks. While threat intelligence sharing is well-established across many sectors, the same is not the case for supplier-related information. Many TPRM teams are open to greater collaboration; however, there remains uncertainty around the legal parameters for such a framework. Greater regulatory guidance in this area may remove these concerns and help enhance sector-wide resilience.

Actions to consider:

- Regulators and financial sector organisations should engage in a dialogue to explore any legal uncertainties that might hinder collaboration.
- Regulators could play a key role in facilitating enhanced collaboration and information sharing among financial institutions. By encouraging industry-wide collaboration, they can enhance the ability of financial institutions to proactively identify and address systemic risks across the sector.



Conclusion



Conclusion

This project proved that collaboration is the key to identifying systemic concentration risks and strengthening the financial sector's resilience. Supply chain risk management cannot be achieved in isolation. Organisations must work together to proactively identify hidden systemic concentration risks and mitigate them before they escalate.

The scale of the findings highlight the power of this approach – despite only six participants, the project uncovered 47 systemic risks across, representing an eightfold multiple relative to the size of the cohort.

This demonstrates that systemic risks are far more widespread than many financial institutions may realise.

If more organisations were to adopt this collaborative approach, the financial sector could significantly improve its ability to detect and mitigate systemic risks.

Regulatory compliance alone is not enough – institutions must adopt a proactive, intelligence-driven approach to third-party risk management, rather than waiting for regulators.

Ultimately, a Defend-as-One mindset is essential. Just as threat intelligence communities (e.g. the Five Eyes Intelligence Community, private sector groups) collaborate to counter evolving cyber threats, greater collaboration within the TPRM community will enable faster threat detection and stronger risk mitigation.

What's next:

- Risk Ledger is exploring the feasibility of a future project that incorporates lessons learned from this pilot and broadens participation to further strengthen collaboration across the industry.
- Risk Ledger will engage with industry associations and financial institutions to explore how to best leverage the insights from this project.
- Risk Ledger is deploying product improvements to address the challenges identified in this project, focusing on supply chain visibility and risk management efficiency. These improvements will include:
    - Faster identification of fourth-party suppliers, enabling quicker mapping of extended supply chains.
    - A streamlined onboarding process to help non-client participants map their supply chains with the same depth and accuracy as existing clients.
    - Enhanced service mapping capabilities allowing organisations to identify the specific services delivered by suppliers, strengthening operational resilience planning.
    - External scanning capabilities to independently validate supplier security assessments, improving risk accuracy and trust in supplier data.

Appendix

About Risk Ledger

Risk Ledger is a pioneering third-party risk management platform that revolutionises supply chain security through a powerful, unified solution. By onboarding and connecting organisations' entire supply chain into an active cyber defence network, Risk Ledger offers a clear view of the entire supply chain. With immediate access to a vast, trusted supplier network and continuously updated risk assessments, Risk Ledger streamlines risk management processes, reduces manual workload, and empowers organisations with unparalleled clarity and control across all supply chain tiers.

Employing a social network-based approach to supply chain cyber security, this enables organisations to leverage their TPRM programmes to gain in-depth contextual insights into the internal security postures of their critical suppliers and achieve enhanced visibility into their extended supply chain ecosystems. It also facilitates collaboration between internal teams, between organisations and their suppliers as well as between industry peers for a more effective and holistic approach to supply chain cyber security.

Each supplier organisation has a profile on the platform, which contains information about their business, but also in-depth assessments of their cyber security controls and other relevant risk areas, including ESG and financial risk. These control questions are based on Risk Ledger's supplier assessment framework, mapped against all leading international standards such as the National Institute of Standards and Technology's Cybersecurity Framework, the International Organization for Standardization's 27001 standard for information security management (ISO 27001) or the UK National Cyber Security Centre's Cyber Security Assessment Framework, optimised for supply chain risk management.

This in-depth profile, controlled by the suppliers, is then shared with their clients with which they are directly connected on Risk Ledger. Clients can set requirements against the assessment framework, as well as label suppliers based on their criticality, whether they hold/handle sensitive company or customer information, have system access and more. Organisations can interact and collaborate with the security teams of their suppliers on remediation and risk mitigation directly on Risk Ledger, building strong partnerships and relationships over time.

Crucially, suppliers are encouraged to also use Risk Ledger to manage their own supply chain risks by connecting with their own suppliers, thus using Risk Ledger as both a supplier and client at the same time. Organisations acting as both suppliers and clients on Risk Ledger is what uncovers the crucial middle links in supply chains and builds the map of interdependencies within the wider supply chain ecosystem. Not just between one client and their third parties, but far beyond.

By facilitating the collaboration and sharing of information with peers in dedicated communities of trusted industry peers, Risk Ledger enables these communities to gain enhanced visibility into shared systemic risks.

Systemic Concentration Risk Details

The table below lists the 47 anonymised suppliers identified as representing systemic concentration risks during the project. As described earlier, the categorisation of these suppliers as a systemic concentration risk is not based on any negative observation of their maturity in managing cyber risk. Instead, it highlights the potential for an outsized impact on the financial services sector should an incident occur, due to the extent of their connectivity across the cohort.

Supplier ID	% of Cohort Connections	Industry/Service Type
Supplier 1	100%	Software and Internet - Cyber Security Services
Supplier 2	100%	Computer and Electronics - IT and Network Services and Support
Supplier 3	66.66%	Computer and Electronics - IT and Network Services and Support
Supplier 4	66.66%	Computer and Electronics - IT and Network Services and Support
Supplier 5	66.66%	Software and Internet - Software Development
Supplier 6	50.00%	Computer and Electronics - IT and Network Services and Support
Supplier 7	50.00%	Software and Internet - Software Development
Supplier 8	50.00%	Software and Internet - Data Analytics, Management, and Internet
Supplier 9	50.00%	Software and Internet - Data Analytics, Management, and Internet
Supplier 10	33.33%	Software and Internet - Data Analytics, Management, and Internet
Supplier 11	33.33%	Computer and Electronics - IT and Network Services and Support
Supplier 12	33.33%	Computer and Electronics - IT and Network Services and Support
Supplier 13	33.33%	Business Services - Accounting, Tax, and Payroll
Supplier 14	33.33%	Business Services - Accounting, Tax, and Payroll
Supplier 15	33.33%	Computer and Electronics - IT and Network Services and Support

Systemic Concentration Risk Details

Supplier ID	% of Cohort Connections	Industry/Service Type
Supplier 16	33.33%	Computer and Electronics - Networking equipment, Network Security, and Systems
Supplier 17	33.33%	Computer and Electronics - IT and Network Services and Support
Supplier 18	33.33%	Financial Services - Other
Supplier 19	33.33%	Financial Services - Other
Supplier 20	33.33%	Software and Internet - Cyber Security Services
Supplier 21	33.33%	Business Services - Other
Supplier 22	33.33%	Business Services - Other
Supplier 23	33.33%	Transportation and Storage - Warehousing and Storage
Supplier 24	33.33%	Business Services - Management Consulting
Supplier 25	33.33%	Software and Internet - Software Development
Supplier 26	33.33%	Business Services - Management Consulting
Supplier 27	33.33%	Software and Internet - Cyber Security Services
Supplier 28	33.33%	Business Services - Management Consulting
Supplier 29	16.66%	Financial Services - Banking
Supplier 30	16.66%	Financial Services - Other
Supplier 31	16.66%	Software and Internet - Cyber Security Services
Supplier 32	16.66%	Telecommunications - Other

Systemic Concentration Risk Details

Supplier ID	% of Cohort Connections	Industry/Service Type
Supplier 33	16.66%	Business Services - Other
Supplier 34	16.66%	Telecommunications - Other
Supplier 35	16.66%	Financial Services - Banking
Supplier 36	16.66%	Financial Services - Banking
Supplier 37	16.66%	Computer and Electronics - Other
Supplier 38	16.66%	Software and Internet - Software Development
Supplier 39	16.66%	Software and Internet - Cyber Security Services
Supplier 40	16.66%	Computer and Electronics - IT and Network Services and Support
Supplier 41	16.66%	Computer and Electronics - IT and Network Services and Support
Supplier 42	16.66%	Computer and Electronics - IT and Network Services and Support
Supplier 43	16.66%	Software and Internet - Software Development
Supplier 44	16.66%	Software and Internet - Cyber Security Services
Supplier 45	16.66%	Computer and Electronics - IT and Network Services and Support
Supplier 46	16.66%	Business Services - Management Consulting
Supplier 47	16.66%	Computer and Electronics - IT and Network Services and Support

RISK LEDGER

Thank you

Risk Ledger transforms third-party risk management by enabling you to onboard and connect your entire supply chain, bringing every supplier into clear view. Access risk insights, mitigate emerging threats, and manage your supply chain with unparalleled confidence - all from a single, powerful platform.

More information can be found on our website https://www.riskledger.com