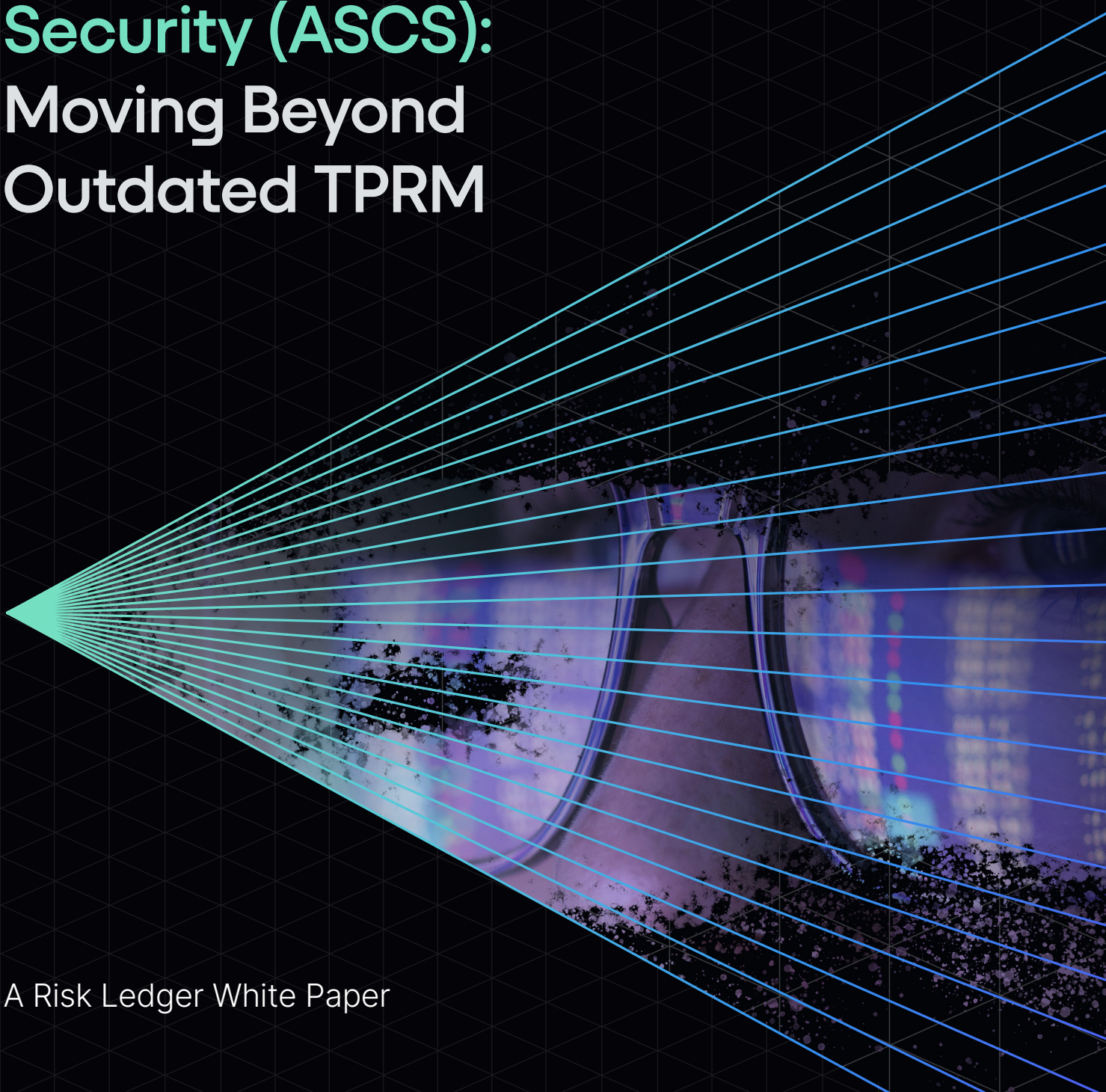
Risk Ledger

Active Supply Chain Security (ASCS): Moving Beyond Outdated TPRM



A Risk Ledger White Paper

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.

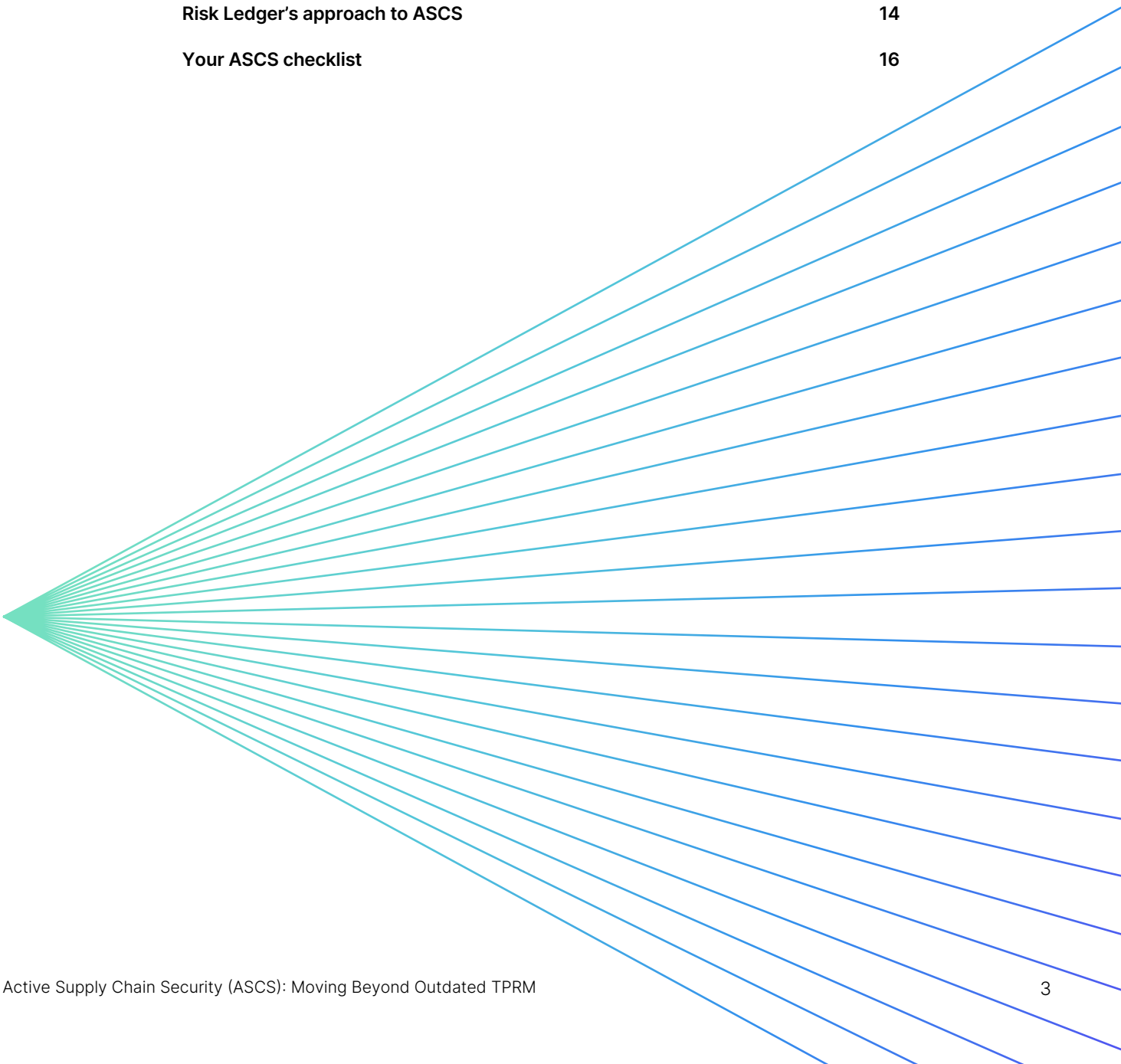
By leveraging network-level insights, ecosystem mapping and emerging threat detection with Risk Ledger, you optimise the entire ecosystem's resources and Defend-as-One.

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

Contents



Introduction

All cyber security approaches have a shelf life.

Just as static perimeter firewalls are obsolete in the era of cloud-connected IoT devices and signature-based anti-virus software is ill-equipped for modern zero-day threats, siloed Third-Party Risk Management (TPRM) is now dangerously outdated in a world of complex, interconnected supply chains.

Traditional TPRM is architecturally flawed

This isn't a feature gap. It's a design problem. Traditional TPRM was created for a simpler world where suppliers were treated as isolated entities, risk was assessed periodically, and compliance was the primary objective. Today's interlinked and risk-exposed ecosystems demand a fundamentally different approach.

- **Supply chains have become the biggest attack surface in cyber security** - 85% of cyber security professionals experienced a supply chain cyber security incident in 2025.
- **AI-powered adversaries are using increasingly sophisticated methods** - 16% of 2025 breaches involved attackers using AI, such as realistic deepfakes and highly-personalised phishing.
- **Obscure nth-party suppliers can bring down an entire ecosystem** - The Log4j cyber incident cascaded through 60% of corporate networks with 800,000 attacks in 72 hours.
- **Cyber security regulations are more demanding than ever** - The EU's Digital Operational Resilience Act (DORA) has shifted focus to active third-party reviews and vendor relationship mapping.

According to the *WEF Global Cybersecurity Outlook 2026*, 78% of CEOs of highly resilient organisations now consider third-party and supply chain vulnerabilities the greatest challenge to cyber-resilience. But, limited by traditional TPRM tools, only 48% map their ecosystem and just 30% share supply chain intelligence with ecosystem partners.

> **"TPRM was built for a simpler world. ASCS is built for today's interconnected and unstable reality. Its unified network-first approach reveals hidden concentration risks, provides nth-party visibility, and enables collective defence across your entire supply chain."**
>
> Haydn Brooks, Co-Founder and CEO, Risk Ledger

Modern supply chain security is a collective defence problem

Today's interconnected supply chains require proactive, coordinated defence, not individual point-solutions. TPRM's static approach, limited visibility, and lack of collaboration are neither fit for purpose, nor fixable with incremental improvements. Instead, a whole new cyber security approach is needed: Active Supply Chain Security (ASCS).

Active Supply Chain Security is the evolution of TPRM for the modern era. It is not a feature upgrade to traditional assurance tools, but a new operating model for supply chain security, built on continuous visibility, shared intelligence, and systemic risk reduction across an interconnected ecosystem.

The result? Security leaders, security analysts and suppliers can move beyond reactive firefighting to proactively strengthen ecosystem resilience and Defend-as-One — because in supply chain security, every link matters.

Architecturally flawed: 5 ways traditional TPRM falls short in the modern era

Traditional TPRM typically involves questionnaires, periodic assessments, and risk scoring to assess risks posed by external suppliers. But this TPRM model no longer delivers the resilience you urgently need — with only 37.2% of UK cyber security professionals considering TPRM "truly effective" in today's threat landscape.

TPRM doesn't fail because teams aren't trying hard enough. It fails because it was built for compliance in a disconnected world, not resilience in a connected one.

1. Point-in-time assessments can't keep up with real-time threats

A supplier's security posture is fluid, not static. A questionnaire submitted on Monday can be irrelevant by Tuesday, so relying on annual assessments leaves your organisation in total darkness for 364 days of the year. What's more, static assessments do not notify you when a supplier's risk profile changes, so you only discover a weakness after it has been exploited.

2. Endless questionnaires waste time and generate incomparable data

Without a unified framework, every supplier fills in hundreds of different security questionnaires for hundreds of different clients in hundreds of different ways. This fragmentation not only confuses and fatigues suppliers — leading to errors and onboarding bottlenecks — but also makes it impossible to compare risk levels across a diverse supply chain.

3. Check-box compliance drains resources without reducing risk

Traditional TPRM delivers 'Compliance Theatre'. It's a box-ticking performance to show regulators you're 'reducing risk' rather than genuine defence. As suppliers can be 100% compliant with a specific framework and still be catastrophically vulnerable to a modern attack, this compliance-first TPRM mindset creates an unwanted cyber security imbalance: maximum assessment effort for minimal security reward.

4. Nth party and concentration risks remain completely invisible

70%

of organisations cannot currently identify concentration risks.

In a modern, hyper-connected economy, your security is only as strong as an obscure company deep in your supply chain. But traditional TPRM only vets your direct third-party relationships, ignoring the vast, invisible web of 4th, 5th, and nth parties that those suppliers rely on. These unseen nth-party vulnerabilities and unidentified concentration risks (i.e. suppliers relying on the same data storage provider) leave you unprepared for cascading supply chain disruptions.

5. Fragmented approach to a shared threat

With traditional TPRM, every organisation is trying to solve the exact same problem, at the exact same time, in total isolation. The current model prioritises self-protection over network resilience, which fails to recognise that a weakness anywhere in the ecosystem eventually becomes a threat to everyone. Then, when a security incident does occur, TPRM's lack of collaboration and shared intelligence prevents successful mitigation and containment.

Sectors most vulnerable to TPRM software limitations

Any sector with vast interconnected supplier networks can suffer from nth-party and concentration vulnerabilities. But if your industry is heavily-regulated and highly-prized by cyber attackers — such as Financial Services, Critical National Infrastructure (CNI) and the Public Sector — then TPRM is leaving you dangerously exposed.

Financial Services

- **Increasing attacks.** 82% of UK financial firms were hit by supply chain attacks in the last 12 months (56% suffered 2+).
- **Obscure nth party threats.** E.g. The data breach at SitusAMC impacted 1000+ downstream financial institutions, including the likes of JP MorganChase and Morgan Stanley.
- **Non-delegable regulations.** It's your responsibility to adhere to the likes of the UK's FCA and PRA Operational Resilience rules (including the Critical Third Party regime), NYDFS 500 and EU's DORA.

Critical National Infrastructure

- **State-sponsored targeting.** 95% of UK CNI organisations suffered a data breach in 2024-2025, with state-supported actors increasingly targeting critical infrastructure.
- **Non-resilient supply chains.** CNI relies on sub-contractors that are traditionally less cyber security-conscious and frequently targeted by cyber attackers (especially the construction industry).
- **Tough new regulations.** Regulators are applying increasing scrutiny to CNI's cyber security resilience, with the UK's Cyber Security and Resilience Bill (2025/2026) raising non-compliance penalties to £17 million or 4% of global turnover.

Public Sector

- **Public Sector in attackers' crosshairs.** The UK National Cyber Security Centre recorded a 130% rise in "nationally significant" cyber attacks in 2025.
- **Complex supply chains.** It only takes one weak link to bring down the entire interconnected Public Sector supply chain, such as CrowdStrike's IT outage's impact on major transport operators.
- **Increasing scrutiny.** For governmental bodies, it's not just regulations that are getting tougher, but also public scrutiny — with the National Audit Office claiming the government does not know how vulnerable its legacy systems are to cyber threats that are 'severe and advancing quickly'.

The ASCS evolution: continuous, collective supply chain defence

Just as modern cloud-based collaboration requires off-premises cyber security, today's interconnected supply chains require collective, coordinated network defence. It's no longer enough to treat suppliers bilaterally — you need to immunise the entire supply chain ecosystem from attacks.

That's why Active Supply Chain Security (ASCS) moves beyond traditional TPRM's static, siloed and compliance-focused approach to deliver:

- **Standardisation at scale.** Share one supplier profile across many clients, creating a common language of risk, improving risk data and eliminating duplicated effort.
- **Network-first visibility.** See your supply chain as it truly exists — a living network of interconnected relationships — not a static list.
- **Continuous monitoring & insights.** Identify concentration risks, nth-party dependencies, and emerging threats in real-time.
- **Collective defence.** Enable security teams and suppliers to work together, sharing intelligence, responding as one ecosystem and building network-wide resilience.

Here's the breakdown of each element in more detail.

First Sentier Investors increased supplier coverage with the same amount of resource by

500%

Active Supply Chain Security is not:

- **Another questionnaire heavy TPRM tool**
- **A superficial external risk rating**
- **A static trust centre**
- **A compliance reporting system**

Active Supply Chain Security is a continuous, network-first supply chain security model that connects organisations and suppliers into a living ecosystem of shared visibility and collective defence.

1. Standardising security assessments

- **One common language of risk.** Standardised assessments create a common language for the entire ecosystem, enabling seamless partner collaboration, efficient security reviews, simplified due diligence and streamlined regulatory reporting.
- **One common profile.** Suppliers maintain a single, standardised security profile, so you can access up-to-date, consistent and peer-validated supplier assessments at any time.

96%

of Security Leaders consider extended supply chain visibility essential for mitigating risks.

- **Faster supplier onboarding.** With all your suppliers on one network, you can assess suppliers instantly with pre-built workflows and standardised processes — reducing onboarding time by over 50%.

2. Visualising the supplier network

- **Network-first supply chain mapping.** With thousands of organisations sharing intelligence on one ever-growing network, you can stop guessing about supply chain dependencies and start mitigating risks.
- **Nth-party visibility.** With the full picture of your nth-tier connections, you can proactively uncover shared dependencies and take action to avoid cascading failures before they happen.
- **Concentration risk insights.** A bird's-eye view of your entire network's concentration risks enables you to make risk-based decisions to mitigate sudden disruptions (i.e. sanctions, policy changes).

3. Continuously identifying threats

- **Continuous risk monitoring.** Receive continuous updates about changes in supplier risk profiles, including cyber security incidents or compliance lapses, so you can respond before any damage is done.
- **Real-time risk signals.** With real-time risk signals, intuitive dashboards and simulated disruptions, you can assess the impact of potential threats, create solid response playbooks and make informed choices around supplier diversification.
- **Emerging threat detection.** By pinpointing emerging threats and potential vulnerabilities, you have time to execute your response plans and get ahead of incidents before they escalate.

Less than

50%

of Security Leaders monitor risks beyond their direct, third-party relationships.

4. Collectively defending the ecosystem

- **Secure collaboration.** By creating a connected community of industry peers, you can share intelligence with network partners, identify common threats and reduce systemic risk across the ecosystem.
- **Proactive incident response.** By leveraging network-level insights, ecosystem mapping and emerging threat detection, your whole industry moves from reactive independent firefighting to proactive united response.
- **Collective defence model.** With your security team working together with industry counterparts, you optimise the entire ecosystem's resources and ensure every link in the chain is fortified.

80%

of the UK water network use the same ASCS platform - improving collective defence.

5 signs your organisation needs ASCS - now

1. Security is a bottleneck when onboarding suppliers

Are you undertaking endless and repetitive security assessments when onboarding new suppliers?

Non-standardised assessments lead to duplicated effort, incomparable security data and onboarding delays. But with ASCS' standardised and centralised supplier assessment processes, you can create a common language of risk, easily compare suppliers' security postures, rapidly verify supplier statements and accelerate supplier onboarding — at scale.

Signs you need ASCS

- **Spreadsheet-based questionnaires for new suppliers**
- **Inconsistent supplier responses**
- **Incomparable security data**

2. Supplier security assessments are updated periodically

Are you relying on third-party suppliers updating their security assessments every 6-12 months?

Long gaps between assessments deliver quickly-outdated security data, leaving you on the back foot for the majority of the year. But with ASCS, your suppliers constantly update one security profile, so you receive real-time alerts to changes in their security posture, identify risks proactively and can plan remediation efforts for emerging threats before it's too late.

Signs you need ASCS

- **Point-in-time assessments Chasing suppliers to update their security profiles**
- **Outdated security questions not aligned to new regulations**

3. Cannot see your supply chain connections beyond 3rd or 4th parties

Are you basing your entire supply chain security on the security postures of your contracted Tier 1 suppliers?

Focusing on third-party suppliers leaves you blind to network concentration risks and exposed to nth-party vulnerabilities cascading through the ecosystem. But with ASCS, map your supplier ecosystem as it truly exists to uncover your hidden nth-party dependencies, track changing supplier relationships, and identify concentration risks shared between your suppliers — at-a-glance.

Signs you need ASCS

- Can't name your suppliers' suppliers
- Unaware of ecosystem concentration risks
- Not tracking suppliers' changing connections

4. Reactive and independent firefighting to third-party breaches

Are you finding out about supply chain breaches from third parties and only initiating defence mechanisms after attacks have occurred?

Waiting to find out about breaches from impacted suppliers is already too late. But with ASCS' continuous alerts and proactive threat management, you get immediate visibility into which suppliers are exposed, how vulnerabilities cascade through your ecosystem and where to prioritise action.

Signs you need ASCS

- No coordinated plan with supply chain partners for breaches
- Not sharing security intelligence with partners
- Waiting until threats reach your door to take action

5. Satisfying compliance regulations but still suffering breaches

Are you achieving certifications and impressing the board with your compliance scores while your security team is still reporting breaches?

Even if you're manually updating your security questionnaire for new regulations, point-in-time compliance audits do not offer sufficient protection for today's rapidly evolving supply chain threats. But with ASCS, you can continually detect real-time threats, free up your security team to remediate emerging risks, and streamline compliance reporting with up-to-date data.

Signs you need ASCS

- Equating compliance with adequate protection
- Using outdated data for reporting
- Championing compliance results in board meetings

Benefits of ASCS for Security Leaders, Security Analysts & Suppliers

Supply chain security is not your business' USP. It's not why you exist, it's not the value you deliver, yet it directly impacts every departmental function (just think of the number of SaaS products in play across your organisation) and keeps security teams up at night.

With traditional TPRM:

Security leaders are worried. 60% of cyber security leaders consider third party supply chain risk "innumerable and unmanageable", so it's no surprise that the leading Security Leaders concerns in 2026 are ransomware attacks, supply chain resilience and exploitation of software vulnerabilities.

Security analysts have their work cut out. While they should be focused on emerging supply chain risks, endless TPRM assessments and compliance reporting fill up their days, with teams taking up to a week to review a single security assessment.

Suppliers are exhausted. Duplicated effort and supplier assessment fatigue has turned security into a roadblock for new business - with security teams drowning in repetitive questionnaire requests and sales teams frustrated at stalling deals.

But Active Supply Chain Security turns the 'unmanageable' into the 'unthinkable': a cyber security framework that bolsters resilience and delivers tangible benefits to security leaders, analysts, and suppliers.

Security Leaders using ASCS get:

- **Board and regulator-ready supply chain intelligence.** The network visualisations and standardised assessment frameworks aligned to regulations provide defensible, audit-ready evidence for board presentations and regulatory reviews.
- **Visibility into concentration risks and nth-party dependencies.** Network-level insights and mapped nth-party relationships enable proactive risk management before they become board-level incidents.
- **Improved team efficiency without adding headcount.** Pre-built workflows and standardised processes reduce manual overhead and accelerate supplier onboarding time by over 50%.

Security Analysts using ASCS get:

- **Continuously updated supplier data on-demand.** Live supplier profiles, standardised data and automated alerts enable faster supplier reviews without duplicated work or manual chasing.
- **Unprecedented visibility into deep tier risks.** Visualising 3rd, 4th, and nth-party connections shines a light on hidden concentration risks and systemic vulnerabilities.
- **An intelligence advantage.** Real-time security updates enable you to identify supplier exposure (and cascading risks) earlier than traditional tools allow, giving you clarity before incidents escalate.

Suppliers using ASCS get:

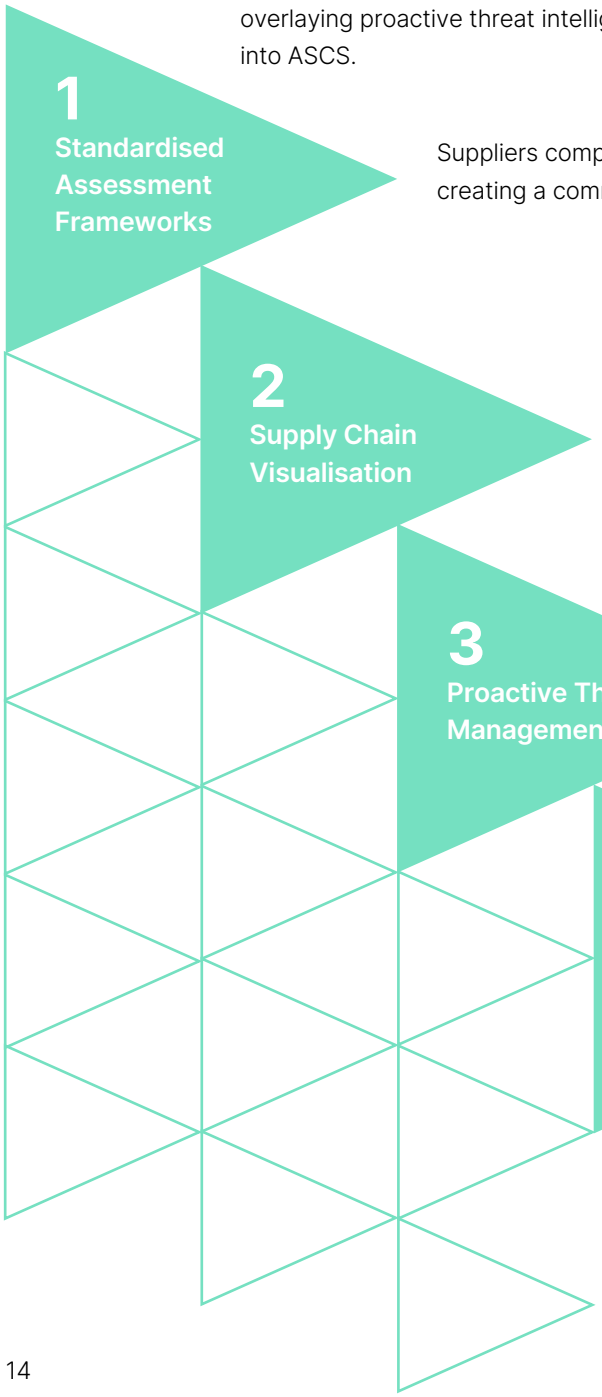
- **Streamlined security assessments.** Instead of answering the same security questions for every client, you complete your profile once and share it with everyone — instantly.
- **Accelerated sales cycles.** Security reviews no longer kill your deal momentum, but help you close faster than competitors.
- **Ahead of emerging threats, not chasing them.** When incidents happen, respond once and reach every client, showing your security leadership.

> "Security leaders, analysts and suppliers working together across the ecosystem is one of the most powerful levers in supply chain security. ASCS supports this coordinated defence while strengthening operational resilience."
>
> Haydn Brooks, Co-Founder and CEO, Risk Ledger

Risk Ledger's ASCS approach

In 2018, Risk Ledger pioneered the network-first approach to supply chain security. Now, we're leading the shift to Active Supply Chain Security.

By standardising supplier data, connecting thousands of organisations onto a living network, and overlaying proactive threat intelligence, our four-stage approach is transforming fragmented TPRM into ASCS.



1 Standardised Assessment Frameworks

Suppliers complete one profile, keep it updated, and share it across the network, creating a common language of risk.

2 Supply Chain Visualisation

We map thousands of organisations, enabling nth-party visibility, concentration risk detection, and shared intelligence.

3 Proactive Threat Management

We overlay new vulnerabilities or attacks on the network map and database in real-time, highlighting impacted suppliers and cascading network exposure, enabling you to prioritise remediation.

4 Defend-as-One

We enable collaboration and intelligence-sharing with the wider ecosystem, optimising resources and building network-wide cyber resilience.

Together, this approach delivers Active Supply Chain Security — continuous visibility, systemic risk reduction, and collaborative defence across complex non-linear supply chains. Because in today's interconnected world, every link matters.

Customer Spotlight: Synetics Solutions

Synectics Solutions is a leading provider of fraud prevention and risk intelligence solutions, trusted by over 160 organisations across financial services and government as their first line of defence.

Challenge: Synectics Solutions' was relying on a laborious, manual TPRM process — based on customised questionnaires and spreadsheets — which was time-consuming and unscalable.

Solution: Risk Ledger's platform enabled Synectic's compliance team to automate supplier assessments, standardise due diligence, and constantly monitor changing supplier profiles, while also delivering far-reaching visibility over their extended supply chain.

Result:

- Clear, auditable records for new FCA compliance rules.
- Seamless risk collaboration between internal teams.
- Cut onboarding time in half.

> "I'd estimate that we spend less than half the time to onboard a new supplier using Risk Ledger than using previous processes."
>
> Steve Sands, Information Security Consultant and Data Protection Officer, Synectics Solutions

Read more...

Your ASCS checklist

For organisations in highly-regulated and targeted industries, Active Supply Chain Security is not an optional TPRM upgrade. It's the difference between costly operational disruptions and seamless value production.

To protect against today's supply chain threats, make sure your organisation:

- [ ] Uses one standardised supplier assessment when onboarding new suppliers.
- [ ] Receives continuous updates and alerts when suppliers change their security posture.
- [ ] Has live visibility of nth-party relationships and concentration risks deep in your supply chain ecosystem.
- [ ] Sees new vulnerabilities emerge in real-time and instantly know who is impacted.
- [ ] Seamlessly collaborates with supply chain partners, sharing threat information and coordinating mitigation action.

In today's interconnected world, security is no longer an individual effort. It requires organisations and suppliers to Defend-as-One — strengthening every link across the ecosystem.

Defend-as-One

Cyber security approaches evolve with the digital threat landscape.

Zero Trust Architectures now protect cloud-connected IoT devices. Endpoint Protection Platforms (EPP) combat today's rapidly evolving zero-day threats. Active Supply Chain Security enables today's interconnected supply chains to Defend-as-One.

Find out how you can enhance your supply chain security with ASCS.

Join the community

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 | marketing@riskledger.com | +44 1234 567890