RISK LEDGER

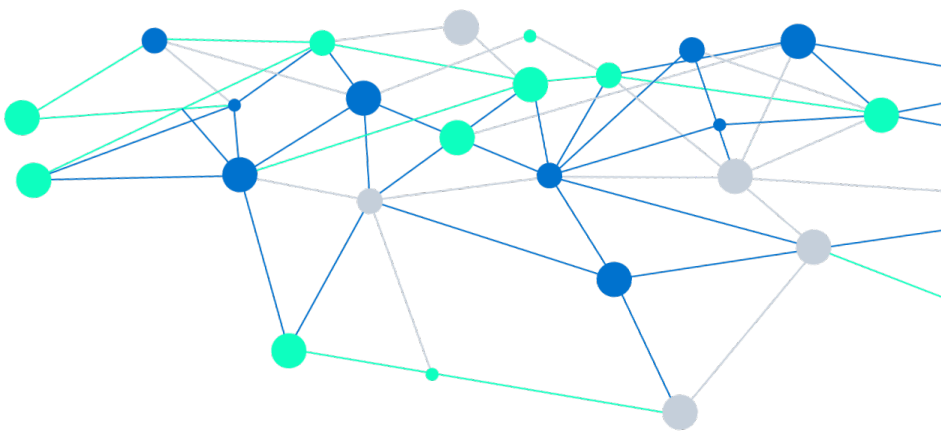
G-Cloud 15

Service Definition

Vendor Risk Management and Supply Chain Security Platform

Risk Ledger

Lot 2b Cloud Software



1. Introduction

Company Overview

Founded in 2018 by Haydn Brooks and Daniel Saul, Risk Ledger exists because supply chain security is a collective defence problem — one that cannot be solved by siloed tools or static processes.

Our mission is to transform Third-Party Risk Management (TPRM) from a compliance-heavy, broken process into Active Supply Chain Security (ASCS): a connected, collaborative approach where organisations and suppliers work together to reduce systemic risk.

By enabling the community to Defend-as-One, Risk Ledger is redefining how supply chains are secured in a world where every link matters.

Value Proposition

Risk Ledger replaces outdated, siloed third-party risk management with Active Supply Chain Security. Our network-first model connects organisations and suppliers through standardised third-party data, creating a common language of risk across the supply chain.

This unified approach reveals hidden concentration risks, provides nth-party visibility, and enables collaborative defence across your entire ecosystem — because every link matters.

Risk Ledger's network is organised into industry-specific communities, enabling organisations facing similar regulatory, operational, and security challenges to collaborate securely. These communities promote shared security standards, reduce duplicated assurance activity, and strengthen collective resilience across sectors.

With Risk Ledger, public sector bodies and regulated industries can:

- Replace static questionnaires with **real-time, standardised assurance**.
- Instantly identify **concentration risks and nth-party dependencies**.
- Receive **proactive alerts** when supplier security controls change or new risks emerge.
- Build a trusted network of suppliers who continuously maintain their security information.
- Engage suppliers through **sector-based communities** that streamline assurance and encourage continuous improvement.

The result: less manual effort, faster supplier assurance, and stronger, more resilient supply chains built through collaboration.

What the Service Provides

The Risk Ledger Supply Chain Security Platform provides a comprehensive, cloud-based service for managing third-party and supply chain security risk through a continuous, network-first approach.

The service replaces manual, point-in-time assurance with Active Supply Chain Security, enabling organisations to continuously assess, monitor, and collaborate with suppliers across their entire ecosystem.

The service provides:

Standardised Supplier Assurance

A standardised TPRM engine that allows suppliers to complete a single, control-based security assessment which can be securely shared across the network. This creates a common language of risk, reduces duplication, and improves data quality.
Assessments map to recognised frameworks including ISO 27001, NCSC CAF, Cyber Essentials, and NIST CSF, and are regularly updated.

Supply Chain Network Visualisation

A real-time view of the supply chain as a connected network, enabling organisations to identify third-, fourth-, and nth-party dependencies, concentration risks, and potential cascading impacts.

Continuous Monitoring

Automatic notification of changes to supplier security controls, removing reliance on annual reviews and enabling proactive risk management.

Collaboration and Remediation

Secure, in-platform collaboration with suppliers to manage remediation actions, share evidence, and track progress, improving accountability and supplier engagement.

Reporting and Governance

Real-time dashboards and configurable reports to support operational oversight, senior leadership reporting, audits, and regulatory engagement.

Public Sector and Regulated Use

Used across UK government, law enforcement, healthcare, critical national infrastructure, and regulated sectors to support compliance, resilience, and operational efficiency.

Secure SaaS Delivery

A fully managed Software-as-a-Service platform with no local installation required, UK-hosted infrastructure, role-based access controls, multifactor authentication, and ongoing maintenance and updates included.

Social Value

Risk Ledger structures its social value programme around six guiding pillars, aligned to the UK Government's Social Value Model. Social value activity will be proportionate to contract size and monitored against clear targets.

Delivery is overseen by an Executive Sponsor (COO or CEO) and Programme Lead (People & Talent Lead).

Across 2026-2029 onwards, Risk Ledger commits to:

Mission: Kick start economic growth

- **Support for SMEs and fair procurement** *(workstreams owned by: Finance and Operations)***:** Maintain ≤30-day payment terms for SMEs and work towards a high proportion of SME invoices paid within 20 days; introduce a Supplier Code of Conduct covering living wage, DEI and environmental expectations; deliver quarterly cyber-basics webinars and enablement sessions for SME vendors; and implement accelerated onboarding and a prompt-payment pledge dashboard, supporting increased spend with SMEs and social enterprises.

- **Innovation for public benefit** *(workstreams owned by: SLT & People)***:** Run a pro-bono pilot offering platform credits or onboarding support to up to three charities or small public bodies focused on cyber resilience; formalise mentoring into startup accelerators and/or VC networks (2-3 active mentorships); release a free "Supply Chain Cyber Starter" resource pack with defined uptake targets; and develop initiatives such as micro-grants and open resources to support SME cyber maturity.

Mission: Make Britain a clean energy superpower.

- **Sustainability and environmental responsibility** *(workstreams owned by: Operations)***:** Measure its footprint using AWS carbon tools and office utilities; refresh and publish an Environmental and Sustainability Policy; identify and prioritise reduction opportunities (e.g. green hosting, developer efficiency, travel and office policies); work towards year-on-year emissions-intensity reduction per employee and per £ revenue; and request emissions and policy disclosures from key suppliers, supported by templates.

Mission: Break down barriers to opportunity.

- **Inclusive employment and fair work** *(workstreams owned by: People & Talent)***:** Maintain Real Living Wage for staff and subcontractors; publish and apply inclusive hiring rubrics and salary bands for ≥80% of roles; move all job ads to skills-based criteria; increase inclusive shortlists (from at least 30% upwards) through targeted outreach; introduce fair scheduling and predictable work policies for contractors; and conduct annual pay equity audits with remediation actions.

- **Skills development and access** *(workstreams owned by: People & Talent with team leads)***:** Maintain role-specific Learning Pathways and a £500 per person learning budget with a target of c.70%+ completion; offer 2-4 paid internships per year across Engineering, Product, Marketing and Customer Success; launch apprenticeship pathways in R&D and commercial functions; operate a mentoring programme (c.10 mentor-mentee pairs); and build an "Academy to Employment" track to convert a growing share of interns and apprentices into permanent roles.

- **Community and charitable impact** *(workstreams owned by: People & Talent):* Run fundraising campaigns linked to employee awards and at least one company-wide volunteer

day; increase volunteer time and funds raised over the period (from c.50 hours and £2k towards higher levels as the organisation grows); expand support to 1-2 additional charities aligned with digital inclusion; provide skills-based volunteering such as cyber clinics for charities and SMEs; and build towards a signature annual event on supply chain resilience with training scholarships.

Mission: Build an NHS fit for the future.

- **Health & wellbeing education** *(workstreams owned by: People & Talent)***:** Build shared understanding of physical and mental wellbeing through practical, low-cost initiatives such as manager training on mental health awareness, stress and workload management, and supporting neurodiverse team members; regular all-hands sessions or lunch-and-learns on topics like burnout prevention and healthy ways of working; and clear internal resources that signpost employees to NHS services and trusted charities for further support.
- **Inclusive employee experience (end-to-end)** *(workstreams owned by: People & Talent)***:** Embed inclusion across the full employee lifecycle by using structured, accessible recruitment processes (clear role criteria, fair interviews, flexibility around reasonable adjustments), inclusive onboarding and induction, and manager guidance on supporting employees with disabilities or health conditions. This includes consistent development and progression frameworks, inclusive performance conversations, and retention practices that focus on flexibility, feedback, and early support rather than reactive interventions.
- **Proactive support for physical & mental wellbeing** *(workstreams owned by: People & Talent)***:** Invest in sustainable, preventative approaches to wellbeing such as training managers to spot early signs of strain, establishing clear expectations around working hours and workload, improving meeting and communication hygiene, and encouraging flexible working where possible. Complement this with wellbeing champions or trained mental-health first aiders, regular check-ins and pulse surveys, and partnerships with free or low-cost NHS-aligned and third-sector organisations to ensure support is accessible to all.

Overview of the G-Cloud Service

Risk Ledger is a cloud-based supply chain security platform that enables organisations to manage, monitor, and strengthen supplier assurance and third-party risk management through a network-first model. Delivered as a Software-as-a-Service (SaaS) solution, it replaces manual, questionnaire-heavy assurance processes with a dynamic, standardised, and collaborative approach.

At its foundation, Risk Ledger provides a standardised TPRM Engine, where suppliers complete one comprehensive security assessment that can be securely shared across the network. This creates a common language of risk that simplifies supplier assurance, ensures data consistency, and significantly reduces administrative effort for both clients and suppliers.

Building on this foundation, Risk Ledger connects thousands of organisations into a living network, enabling them to see and understand the relationships, dependencies, and potential risks that exist across their supply chain. This unique network-first model transforms assurance from a one-way compliance exercise into a shared, collaborative process that drives continuous improvement.

The platform delivers Active Supply Chain Security (ASCS) — continuous, collaborative, and systemic defence across the entire supply chain. This means organisations can:

- Gain complete visibility of suppliers and nth-party dependencies.
- Identify concentration risks and shared dependencies that could impact resilience or service continuity.
- Receive proactive alerts on new or emerging vulnerabilities that may affect their suppliers.
- Engage suppliers directly within the platform to manage remediation and share updates securely.
- Access real-time insights and generate board-ready reports aligned to frameworks such as NCSC, ISO 27001, DORA, and Cyber Essentials.

Risk Ledger helps organisations move from reactive compliance to proactive security by providing real-time intelligence, visualisation tools, and standardised data — reducing risk while improving operational efficiency.

How it Works

1. Onboard and Connect:
   Clients invite suppliers to join the platform. Suppliers create a single, standardised profile that can be shared with multiple clients, reducing duplication and assessment fatigue.
2. Assess and Visualise:
   The platform automatically maps relationships across the supply chain, visualising dependencies, shared suppliers, and potential concentration risks.
3. Monitor and Act:
   Continuous updates and live threat intelligence overlay allow organisations to see how emerging vulnerabilities may impact their suppliers or broader ecosystem.
4. Collaborate and Improve:
   Clients and suppliers can communicate directly within the platform to manage remediation actions, track progress, and build stronger, trust-based relationships.

Associated Services

All maintenance, alerting (phone and email), and data storage are included as part of our standard service pricing.

Additional Modules and Add-ons are available to enhance the functionality of the standard Risk Ledger Enterprise licence. Options include:

- External Monitoring
- Additional Users & Suppliers
- Additional Domains, including:
    - Financial Risk
    - ESG
    - UK Government Data & Personnel Security

Pricing details are provided in the pricing document.

All standard support, maintenance, and customer success services are included in the licence cost.

2. Data Protection

Information Assurance

We are certified to Cyber Essentials, and to ISO27001 through BSI. We have a full suite of security policies covering network security, application security, physical security, HR security, and many other domains, as well as a full suite of BCP and incident response plans, and a dedicated information security owner.

We undertake regular security testing of our web application and infrastructure through CREST accredited penetration testing firms that we rotate periodically. We undertake a full security assurance programme over our suppliers, using our own Risk Ledger Supply Chain Security Platform to do so.

Our application is monitored for security events and all events are triaged and investigated. More details of our extensive security programme can be provided to the buyer on request.

Data Back-Up and Restoration

All data on the platform is automatically backed up daily and weekly as per our backup schedule. Our backup process is reviewed annually.

All backups are encrypted using AES 256-bit encryption, and backups are stored in different geographic data centres to our production environment to provide redundancy.

Backups are tested quarterly to ensure integrity in line with our backup policy.

Business continuity statement/plan

We have a full incident response, IT disaster recovery, and business continuity programme in place which is tested annually. Our system has been built with redundancy to minimise downtime. Our business continuity plan identifies critical functions of the business (e.g., our production hosting environment, payroll etc.), acceptable downtime for each, and outlines plans to maintain operations if a disaster were to take place. A more detailed plan can be provided to the buyer on request.

Privacy by Design

We do not collect large volumes of personal data, we only collect the names, business email addresses, mobile numbers (for 2FA), and IP addresses of the users of the platform. We fully comply with GDPR and have multiple layers of security built into the platform, which undergoes regular independent security testing.

We are certified to Cyber Essentials and ISO27001. Our application is monitored for security events. More details of our extensive security programme can be provided to the buyer on request.

3. Using the service

Ordering and Invoicing

Please email **sales@riskledger.com** confirming you intend to award a **G-Cloud Call-Off Contract** to Risk Ledger (or if you require any clarification on this Service Definition). If available, include your **Lot**, **Service name/ID**, and a **commercial contact**.

Process

1. **Requirements call:** We'll schedule an initial call to confirm scope, users, timelines, and any dependencies.
2. **Order form & Call-Off:** We'll document the agreed scope and pricing in an order form for countersignature alongside your Call-Off.
3. **PO & provisioning:** On receipt of your **purchase order (PO)** and executed Call-Off, we'll provision your tenant and admin users.
4. **Onboarding:** Your **Customer Success Manager** will guide setup, training, and go-live, and remain your ongoing point of contact.

Invoicing

- Invoices are issued to the contracting authority and reference your **PO** and **Call-Off** details.
- Billing follows the schedule agreed in the order form (e.g., **annual in advance**) and aligns with standard public-sector payment terms (**30 days**) unless otherwise agreed.
- **Maintenance, alerting (phone/email), and data storage** are included within standard pricing—no hidden fees.

For any questions at any stage, contact **sales@riskledger.com** and we'll help immediately.

Availability of Trial Service

A free trial is available for a limited number of users and features, with a restricted number of supplier connections. Trials typically run for two weeks, with the exact duration agreed on an individual basis.

Pricing Overview

Risk Ledger Enterprise: The Enterprise package is designed for businesses managing hundreds of suppliers across global teams. It features plus expanded scale, priority support, and dedicated success management—empowering your team to confidently secure your extended supply chain at speed and scale.

What does the licence include?

The **Risk Ledger Enterprise licence** provides full access to the platform's capabilities and enterprise-grade support, designed for organisations managing complex or large-scale supplier ecosystems.

Each Enterprise licence includes:

Platform Access

- Unlimited access to the **Risk Ledger SaaS platform**, hosted securely in the UK.
- Designated **Admin Users** and flexible additional user roles to support security, risk, and procurement teams.
- Access for suppliers at no additional cost — suppliers join and maintain their profiles free of charge.

Core Capabilities

- **Standardised TPRM Engine** – Collect, assess, and manage supplier assurance data through a single, standardised framework.
- **Network Visualisation** – Map supply chain dependencies, concentration risks, and nth-party relationships in real time.
- **Continuous Monitoring** – Receive proactive alerts for vulnerabilities, incidents, and emerging threats across connected suppliers.
- **Collaborative Workflows** – Communicate with suppliers directly within the platform to manage remediation and evidence updates.
- **Reporting & Analytics** – Generate custom dashboards and exportable reports aligned to frameworks such as **ISO 27001**, **NCSC CAF**, and **DORA**.

Support & Success

- Dedicated **Customer Success Manager (CSM)** for onboarding, best-practice enablement, and ongoing optimisation.
- Access to Risk Ledger's **UK-based support team**, available via email, phone, and in-platform chat.
- **Maintenance, phone and email alerts, and data storage** all included within standard Enterprise pricing.
- Access to the **Defend-as-One** community for collaboration, knowledge sharing, and supplier engagement.

Updates & Enhancements

- Continuous platform enhancements and feature updates, automatically included with the Enterprise licence.

On-Boarding, Off-Boarding, Service Migration, Scope

On-Boarding

Each client is assigned a **dedicated Customer Success Manager (CSM)** who will organise an onboarding meeting and share our step-by-step onboarding guide.

Getting started is simple - signing up takes around five minutes, after which your organisation can begin connecting with suppliers immediately.

Your CSM will support you throughout setup and supplier engagement. Depending on the number of suppliers to be reviewed, the CSM can assist with **bulk invitations and connection requests** at no additional cost. This service is available on request at any time during onboarding.

Off-Boarding

Clients should provide 30 days' written notice prior to the end of their contract to begin the off-boarding process.

At the end of the notice period, your account will be suspended and access to the platform will cease. You will be provided with a full export of your data in CSV format.

The off-boarding process, including timelines and export outputs, can be tailored in agreement with your CSM. All client data is securely deleted within 60 days of account suspension in line with our data retention policy

Training

Your **Customer Success Manager** provides virtual onboarding and platform training sessions for your team.
In addition, clients have access to:

- A detailed **onboarding and training guide**;
- Our **in-house security consultant**, who can support the embedding of your Third-Party Risk Management process; and
  An extensive **online knowledge base** and help centre.

All training and documentation are included at no additional cost.

Implementation Plan

A detailed implementation plan can be provided upon request.
As Risk Ledger is a **Software-as-a-Service (SaaS)** platform, setup is quick and straightforward - most clients are fully operational within minutes.

The process involves:

1. Completing a short online registration form to create your account (including secure login and two-factor authentication).
2. Connecting with your suppliers immediately upon login.

Service Management

Risk Ledger operates a **Continuous Integration/Continuous Deployment (CI/CD)** development model, ensuring regular updates without service disruption.

We maintain an average uptime of **99.9%**, exceeding our contractual KPI of **98% uptime**.
If scheduled maintenance is required, clients are notified in advance in accordance with the minimum notice periods defined in **Appendix 1, Clause 2** of our terms.

Service Constraints

- Risk Ledger currently operates at **99.9% uptime**, above the defined SLA threshold.
- **All scheduled maintenance** is conducted outside UK business hours and communicated in advance.
- There are **no other service constraints**.

Service Levels

Risk Ledger's minimum service levels are defined in our **standard terms**, but these can be adjusted to meet client-specific requirements and documented in the **Order Form** during the Call-Off stage.

Outage and Maintenance Management

Risk Ledger follows a robust **Software Development Lifecycle (SDLC)** with rigorous testing, rollback plans, and change control for every deployment. Downtime and performance are continuously monitored through our cloud application monitoring tools.

All deployments are performed outside business hours to minimise service impact.

Financial Recompense Model for not Meeting Service Levels

Availability in relevant month	**Service Credit**
98% and above	None – meets expectations
Between 95% — 98%	5% reduction in annual charges payable for the relevant month
95% and below	10% reduction in annual charges payable for the relevant month

4. Provision of the service

Customer Responsibilities

You are obligated to ensure that your Authorised Users shall not:

- use the Services, Materials or Participant Data in any way so as to bring Risk Ledger or any other party into disrepute.
- use the Services, Materials or Participant Data in a manner which is unlawful, harmful, threatening, abusive, harassing, tortious, indecent, obscene, libellous or menacing.
- use the Services, Materials or Participant Data in a manner which infringes the Intellectual Property, proprietary or personal rights of any third party, including data subjects.

- misuse the Site or Software by introducing viruses, trojans, worms, logic bombs or other material which is technologically harmful.
- attempt to gain unauthorised access to the Site, Software or Services, the server on which the Site, Software or Services are stored, or any server, computer or database connected to the Site, Software or Services.
- attack the Site, Software or Services via a denial-of- service attack or a distributed or malicious denial-of service attack.
- access the Software, Services or the Site in order to build a product or services which competes with the Software, Site or Services.
- use the Services, Materials or Participant Data, or disclose them to third parties, except as authorised in writing by Risk Ledger or as permitted under Risk Ledger's terms.

You are obligated to keep passwords and other access details for use with the Services confidential and restricted to those members of staff who need to know such details. You shall ensure all such staff are aware of the confidential nature of such information and treat it accordingly. You shall notify Risk Ledger immediately if it believes that such information is no longer secret. Your organisation is solely responsible for all activities that occur using the Organisation's authentication credentials.

You will take all reasonable steps to ensure that nobody other than Authorised Users accesses the Services using Authorised User accounts. Authorised User accounts may not be shared between individuals. Clients may have up to the number of Authorised Users stated on the Order Form.

Technical Requirements and Client-Side Requirements

Risk Ledger is a **cloud-based Software-as-a-Service (SaaS)** platform delivered through a secure web interface.
There is **no installation or local infrastructure** required — the service is fully hosted and maintained by Risk Ledger.

The platform is compatible with all **modern, up-to-date, and supported web browsers**, including:

- Google Chrome
- Microsoft Edge
- Mozilla Firefox
- Apple Safari

  Note: Internet Explorer is not supported.

Users require a stable internet connection and access to a supported browser. There are **no additional technical prerequisites, plugins, or client-side software** needed to use the Risk Ledger platform.

Development life cycle of the solution

Risk Ledger follows an agile development process with frequent incremental releases. Our customer success team and product team work together to define what problems our clients would like to solve, to collect feedback on the platform, and use this to build and influence our development roadmap.

Once feedback or a suggested feature is proposed by a client, our customer success team will engage our product team to enter it in our roadmap. Once in our roadmap, the feature will have a proposed date for shaping, which is the next stage in the process. Shaping (approximately 1 week) is when our product team will contact the customer to find out more about the problem they are trying to solve, and to define the solution or feature to solve it.

Once shaped, the feature then enters technical design (approximately 1 week), which is where the feature's implementation is designed from a technical perspective. After this, the feature will have a release date and will be built and implemented into the platform in line with this. Customer success will then re-engage the client to collect feedback on whether the problem has been solved or not.

After-sales Account Management

Every **Risk Ledger** client is supported by a **dedicated Customer Success Manager (CSM)**, backed by our **UK-based support and technical teams**.

Support is available via **email** and through the **in-platform Help Centre**, which includes an extensive knowledge base, troubleshooting guidance, and product updates.

Your Customer Success Manager provides:

- **Best-practice guidance** on optimising supply chain security and assurance processes.
- **User training and onboarding support** to accelerate adoption and value.
- **Ongoing performance reviews** to identify opportunities for efficiency and improvement.

To ensure continued alignment with your objectives, we conduct **Quarterly Business Reviews (QBRs)** to assess progress against your defined goals, track platform usage, and ensure overall customer satisfaction.

Termination Process

Approximately **60 days before the end of the contract**, your **dedicated Customer Success Manager (CSM)** will contact you to discuss renewal options and confirm your ongoing requirements.

Clients may terminate their agreement by providing **no less than 30 days' written notice** to their CSM, who will coordinate the termination and off-boarding process.

The customer acknowledges that it has purchased the Services for the **Minimum Period** (and any **Renewal Term(s)**) as defined in the **Order Form or Certificate of Purchase**.

Following termination, Risk Ledger will ensure a smooth off-boarding process, including data export and secure deletion in line with our retention policy.

5. Our experience

Case Studies

NHS Test & Trace / NHS England (client since March 2021)

Sector: Healthcare / Public Sector
Use Case: Supply Chain Security and Continuous Supplier Assurance

NHS Test and Trace (now part of NHS England) provides a critical national service that is both technically and logistically complex, relying on a large network of specialist suppliers. To secure this supply chain and ensure operational resilience, NHS Test and Trace implemented the Risk Ledger Supply Chain Security Platform.

Managing supplier assurance manually was time-consuming and made it difficult to identify hidden vulnerabilities or shared dependencies across suppliers. The organisation needed a solution that could scale rapidly, automate risk assessments, and provide real-time visibility across their supply chain.

Using Risk Ledgers standardised assessment framework and network visualisation, NHS Test and Trace gained detailed, control-based insights into each supplier's security posture. During their initial review, they identified that one of their essential suppliers was exposed to a large-scale, non-targeted malware attack.
As the supplier provided a critical, specialist service, replacement was not an option. Instead, NHS Test and Trace's security experts used the Risk Ledger platform to collaborate directly with the supplier, helping them strengthen their defences and remediate the identified risks.

Risk Ledger's Network Visualisation also revealed that one critical supplier was directly connected to two other suppliers, creating a concentration risk. With this visibility, the NHS Test and Trace team proactively worked with all three suppliers to address the interdependencies and prevent potential cascading disruption.

Outcome
Through the Risk Ledger platform, NHS Test and Trace was able to:

- Secure its supplier ecosystem more effectively and collaboratively.
- Gain continuous visibility of supplier risk and shared dependencies.
- Streamline assurance through automation and a standardised process.
- Strengthen resilience across critical national infrastructure.

"We wanted something automated and efficient that would scale quickly and could be applied to multiple use cases."
— Mark Logsdon, CISO, NHS England

City of London Police (client since April 2020)

Sector: Law Enforcement / Public Sector
Use Case: Supply Chain Visibility and Collaborative Risk Management

The City of London Police (CoLP) is responsible for information security across three key domains — the City of London Police, the City of London Corporation, and the National Cybercrime Reporting Centre. Given the critical nature of its operations, CoLP must manage a complex supplier network and maintain assurance not only over its direct suppliers but also across connected third and fourth parties.

The primary challenge for the City of London Police was the inability to see beyond its immediate suppliers — to identify hidden interdependencies and systemic risks that could affect operational resilience. Traditional methods provided only a narrow view, limiting visibility into how suppliers interacted or where cascading risks might emerge.

The City of London Police adopted the Risk Ledger Supply Chain Security Platform in April 2020 to strengthen its supply chain security and gain a holistic view of supplier risk.

Using Risk Ledger's Network Visualisation capability, the Information Security team can now map supplier relationships and dependencies, identify potential points of concentration, and collaborate directly with suppliers to mitigate risks.

The platform also enables joint working between security and procurement teams, allowing them to manage supplier onboarding, assurance, and ongoing risk oversight from one central location. With up-to-date data and a shared risk view, the Director of Information Security can brief the Chief Officer Team with clarity and confidence, highlighting focus areas for improvement and promoting good practice across the supply chain.

Outcome
Through Risk Ledger, the City of London Police has been able to:

- Gain deeper visibility of supply chain interdependencies and systemic risk.
- Streamline collaboration between security and procurement functions.
- Enhance reporting and communication with senior leadership.
- Improve the efficiency and impact of supply chain risk management using technology.

"It's really about the capability to match the growing demand of supply chain security risks with limited resources, and we can offset that by using technology more intelligently — which Risk Ledger allows us to do."
— Gary Brailsford-Hart, Director of Information Security, City of London Police

Cheshire Police (client since April 2020)

Sector: Law Enforcement / Public Sector
Use Case: Regulatory Compliance and Continuous Supplier Monitoring

Cheshire Constabulary was preparing for an upcoming Information Commissioner's Office (ICO) audit and needed to demonstrate robust third-party risk management (TPRM) and regulatory compliance. The IT Security team also wanted to strengthen collaboration with procurement and implement a more efficient, continuous approach to monitoring supplier security — replacing time-consuming, manual processes.

Before adopting Risk Ledger, Cheshire Constabulary's TPRM process relied heavily on spreadsheets and manual document sharing, making supplier assurance labour-intensive and resource-heavy.

Budget constraints meant expanding the team was not an option, and leadership needed a scalable solution that would automate supplier assurance while aligning to best-practice security frameworks.

Cheshire Constabulary adopted the Risk Ledger Supply Chain Security Platform to automate third-party assurance and achieve real-time supplier visibility.

Using Risk Ledger's standardised assessment framework, mapped against leading standards such as ISO 27001, NIST CSF, NCSC CAF, and Cyber Essentials, the team could easily assess supplier security and regulatory alignment. The framework is updated every six months, ensuring compliance with emerging requirements without internal overhead.

The platform's Network Visualisation enabled the IT and procurement teams to collaborate on supplier risk management in one shared environment. Supplier information — covering security, privacy, financial resilience, and environmental policies — is accessible from a single dashboard, allowing teams to review, filter, and act quickly.

With continuous monitoring, Cheshire Constabulary now receives automatic alerts when a supplier's security controls change, ensuring early visibility of potential risks or compliance gaps.

Outcome
By implementing Risk Ledger, Cheshire Constabulary has been able to:

- Demonstrate best practice in third-party risk management for ICO audits.
- Enhance collaboration between security and procurement teams.
- Automate assessments and save significant administrative time.
- Continuously monitor suppliers and respond proactively to control changes.
- Access regularly updated, standards-aligned assessments without manual maintenance.

"If a supplier decided, for example, to start using a data centre in a problematic jurisdiction, we didn't have any visibility of that unless they told us. The benefit of Risk Ledger is that we are now informed automatically if an important security control like this changes."
— Stuart Rogers, Head of IT & Information Security, Cheshire Constabulary

Case Study: Civil Aviation Authority (client since May 2021)

Sector: Aviation / Regulator
Use Case: Supplier Assurance, Automation & Continuous Monitoring

The Civil Aviation Authority (CAA) is the UK's independent aviation regulator. To strengthen assurance across a complex supplier ecosystem, the CAA set out to transform third-party risk management; moving from manual, point-in-time checks to an automated, continuous, and collaborative model.

Legacy, manual assurance processes were time-consuming, fragmented, and offered limited visibility of downstream dependencies or security control changes across suppliers. The CAA wanted to automate onboarding, be notified of control changes, and gain an up-to-date overview of supplier controls at scale.

The CAA implemented Risk Ledger to centralise supplier assurance and enable continuous oversight. Using Risk Ledger's standardised assessment framework (mapped to ISO 27001, Cyber Essentials, NIST CSF, and NCSC CAF) and Network Visualisation, the CAA harmonised assessments, improved cross-team collaboration, and gained live visibility across its supplier network.

"I'll be honest. This is probably a better tool than any other tools that I have used."
— Matangi Patel, Information Security Officer, Civil Aviation Authority.

Outcome

- Automation & efficiency: Supplier onboarding and assessment workflows are streamlined; the team receives automatic alerts when supplier controls change.
- Visibility & reporting: A consistent, control-based view enables faster analysis and clearer stakeholder reporting.
- Resource impact: Time saved equates to more than a full-time role compared with previous methods.

"The amount of time it would've taken to do what Risk Ledger does… is more than a full-time hire's work."
— Matt Taylor, Chief Information Officer, Civil Aviation Authority.

Clients

Contact Details

Alex Lyma-Young
Sales Director
sales@riskledger.com
+44 20 3488 5800