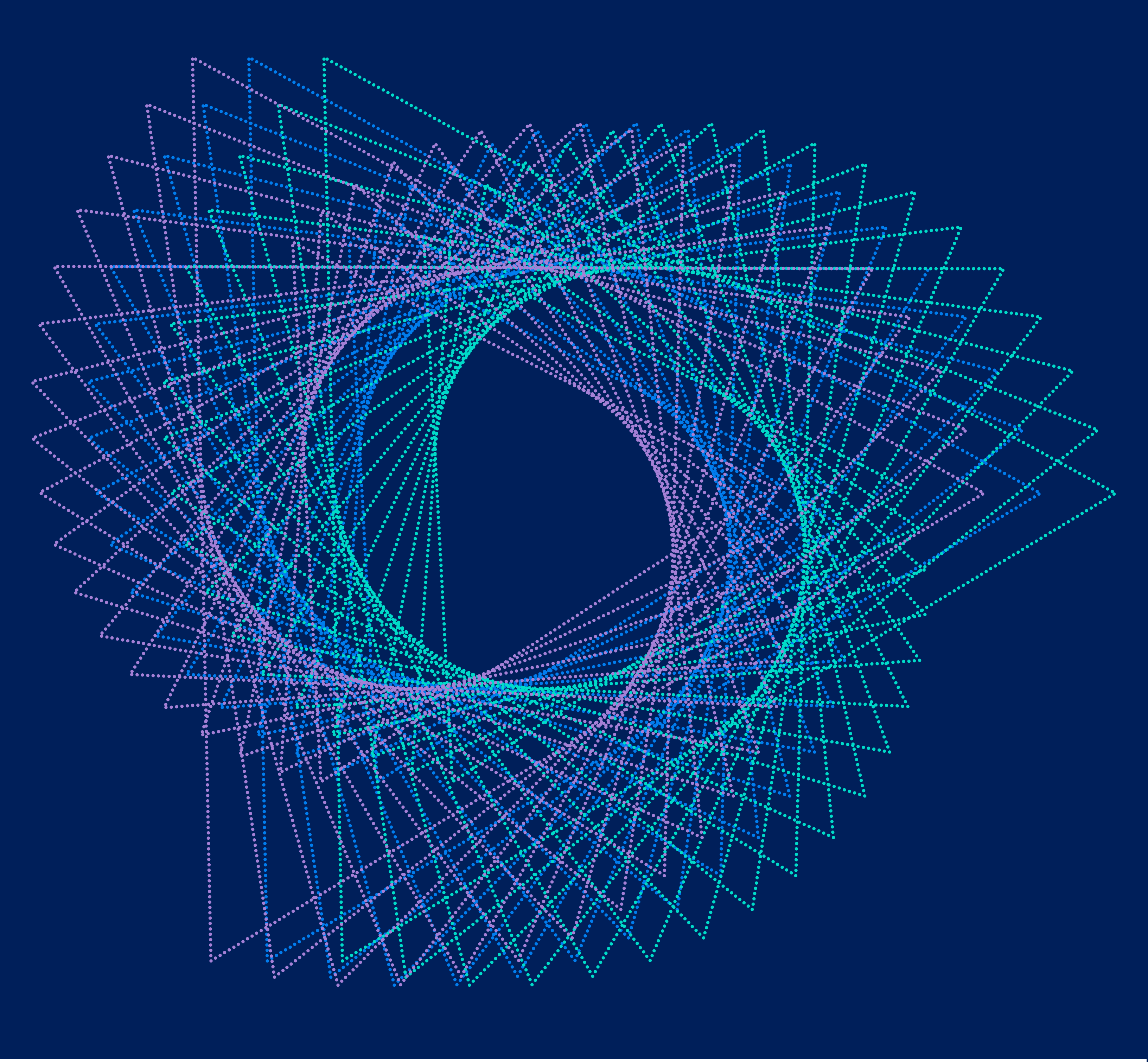


Why AI is Now Risk Leaders' Secret Weapon

levelpath

TABLE OF CONTENTS

Artificial intelligence adoption is creating a dual reality for organizations: new supplier risk challenges that demand attention, paired with innovative technological capabilities that can address these very issues. Smart enterprises are using AI to strengthen their supplier oversight while adapting to new operational models.

Introduction

The rise of artificial intelligence (AI) has affected all organizations, and AI supplier risk management is becoming a critical priority as adoption accelerates. According to McKinsey's The State of AI survey, released in March 2025, 78% of respondents say their organization uses AI in at least one business function, up from 72% in early 2024 and 55% in 2023.

AI is now being widely deployed across businesses and functions, with the most common applications in IT, marketing and sales, and service operations. IT saw the biggest increase in deployment, with the number of functions saying they use AI rising from 27% to 36% over the six months covered by the survey.

In the race to embrace the benefits of AI, businesses face new considerations about additional risks. AI increases the reliance of organizations on IT systems, potentially exposing them to additional cyber-risks and enhancing the potential damage that can result from a successful attack. There are also legal risks around both data protection and how data is used, with many organizations still struggling to formulate a clear governance position.

The risks from AI are enhanced by the wider supply chain, where businesses inherently have less control. A recent survey by Gartner reveals that only 23% of supply chain leaders have a clearly defined AI strategy in place across their organization while 30% have no AI supply chain strategy at all.

"AI is changing how organizations think about supplier risk. It is not just about avoiding problems, but about creating smarter, more proactive ways to manage contracts and data. With the right approach, AI gives legal, risk, and compliance leaders greater visibility and control than ever before," explains Stan Garber, Co-founder and President of Levelpath.

78%

of respondents say their organization uses AI in at least one business function

Source: McKinsey State of AI survey

Business Data in Supplier Contracts

One major risk for organizations, in addition to both legal and supply chain professionals, is the potential for business data to be used by software suppliers, as they attempt to improve their own AI capabilities. The McKinsey State of AI report finds 36% of organizations now use AI in software engineering, and with a race to gain competitive advantage, there is significant potential for data to be used by suppliers in ways that were not acceptable to the owner of that data.

It is an issue that is front of mind for Meg Kociemba, Senior Director at the Office of the Chief Information Officer at US building contractor Suffolk. "We, and most companies, have generally looked very closely at how data is handled in the traditional sense, such as whether it is anonymized before it is used for any data aggregation," she says.

"With the introduction of AI, we need to be very mindful about how data is being used, such as whether it is being used to train a third-party model. We did not really have to worry about a company training their own model three four years ago, because it cost millions of dollars. Now a kid with a laptop and $200 can train a model, and that is something that concerns me, particularly when we lock ourselves into longer-term contracts," says Kociemba, underscoring why organizations need stronger AI procurement governance.

As a general contractor, Suffolk can have as many as 150 active construction sites, with each project having access to sensitive information that is the property of its end-client. "We are taking that owner's proprietary data, designs and models onboard in our systems, and we are stewards of that data," she adds. "This is not our data to give away."

For example, Suffolk is currently working on a uniquely shaped building design. "What if that design gets fed into an AI tool, and all of a sudden a competitor of our client constructing another building gets that same design presented to them?" she says. Other contracts are in high-risk environments such as airports, which are covered by the Patriot Act, meaning breaches of information cannot happen.

> "
>
> We, and most companies, have generally looked very closely at how data is handled in the traditional sense, such as whether it is anonymized before it is used for any data aggregation."
>
> – Meg Kociemba,
> Senior Director
> Suffolk Construction

36%

of organizations now use AI in software engineering

McKinsey & Company

All this means contracts are coming under far more scrutiny by the legal team, with software vendors treated similarly to sub-contractors who represent Suffolk. "We send a questionnaire out to vendors and, from there, we route it to our information security team to review," says Kociemba. "Then it also goes for a risk analysis and an architecture review to make sure that we can integrate it into our ecosystem efficiently, safely, and maintain data security."

The business then uses Levelpath's AI procurement platform to make sure its legal team has access to all relevant information. Levelpath does not use customer data to train its models, ensuring that Suffolk's security needs are met. "That allows us to put the proper protections in place when we get to the contract phase," says Kociemba. "It has been a wake-up call for people in my organization, because I need to make sure that we have the protections in place for our data and our systems."

Where Traditional Risk Management Falls Short

It is not just data being used for unintended purposes that is a threat for those in charge of suppliers, risk, and contract management. Jim O'Rourke, who has served as Chief Procurement Officer at Vanguard, Conagra Brands, and TreeHouse Foods, identifies several additional risks that supply chain professionals and lawyers need to be aware of:

AI model relevance:
This could become an issue over time, says O'Rourke, especially if using a platform that is not AI-native. "Bolt-on AI platforms may not be truly agentic and that can cause drift from better decision-making and adaptation as business cases evolve," he says.

Viability risk:
There are several new and disruptive players in the AI market, says O'Rourke, and not all solutions perform consistently or reliably. "Some AI platforms may struggle with accuracy issues, including hallucinations or inconsistent outputs that don't meet enterprise-grade requirements," he explains. "If a company chooses a supplier whose technology proves unreliable or fails to deliver promised capabilities over time, the organization could face declining performance, user frustration, and the costly need to migrate to a more dependable solution," he warns. "This creates both operational disruption and potential compliance risks if the AI system's unreliability affects critical business processes."

Rogue early adopters:
this can happen when people in an organization begin to use an AI tool that has not been cleared through a governance process, creating vulnerabilities as well as information leaks. "A contemporary example of this risk emerged with early cloud collaboration platforms," says O'Rourke. "Organizations discovered employees were using unsanctioned file-sharing services to collaborate on sensitive projects, inadvertently exposing confidential information through default public sharing settings or inadequate access controls."

57%

of organizations have a fully centralized approach towards risk and compliance when it comes to the use of AI

McKinsey & Company

13%

rely on a fully distributed arrangement, where individual users, sites, or companies determine their own level of acceptable risk

McKinsey & Company

Four Ways Organizations Unknowingly Create Their Own Risk Crisis

O'Rourke identifies common obstacles many organizations face when trying to get visibility into risks that exist across enterprises:

Operating in silos: Master data dependency creates silo behavior where one function solves "their" problem and creates adverse consequences for others. "An example would be a minimum order quantity for a packaging item in a procurement supplier portal that is dynamic, and does not refresh when the supply and demand planners update their sales and operations planning forecast," he says.

Failing to establish AI governance: Organizations struggle when compliance policies fail to offer clear guidelines and controls for third-party AI tools that can be easily accessed through a browser. "This requires a different approach than managing an IT platform that can be controlled with administrative rights, where installation can be prevented if needed," says O'Rourke.

Misunderstanding AI capabilities: Many leaders lack understanding about what AI is and how it can be implemented to increase efficiency, accuracy and decision-making for an organization. "Currently there is a lot of fear regarding what AI is and what it is not," he says.

Excluding IT from AI decisions: Organizations fail when they do not involve IT or legal teams when using software as a service that employs AI. "IT should be engaged early in the discussion, and the discovery and research of potential platforms and suppliers should be included in their annual plan to account for resources required to do the proper due diligence," he says. "Similarly, legal resources should be engaged early in the process to avoid last-minute hurdles."

These risks underscore that enterprises cannot rely on traditional, check-the-box processes to protect themselves. As Dr. Eloise Epstein, a partner at Kearny, puts it, “risk is about setting the right culture. Alignment, approach, and workflow is ‘check the box’ busywork to make us feel like we are productive, when in fact these activities make us less secure because it creates a false sense of protection.”

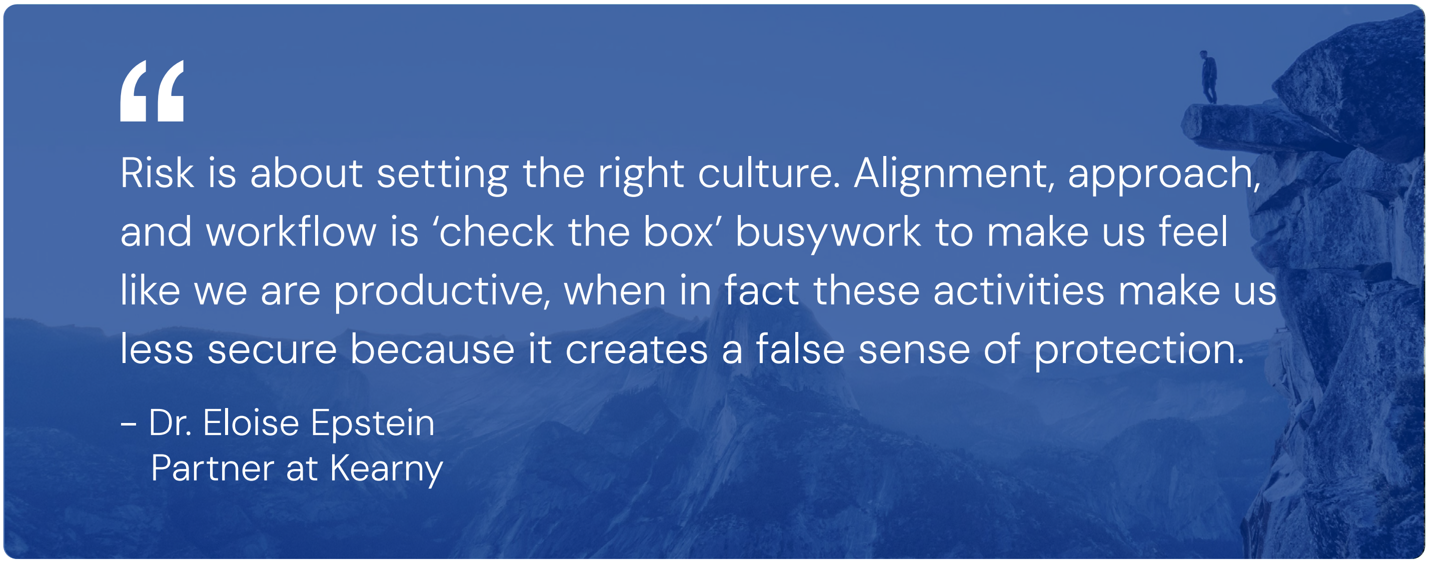
This perspective reframes supplier risk management as more than a procedural exercise. It demands that leadership teams treat risk as an operating principle woven into daily decision-making, not as a one-time hurdle cleared at onboarding.

McKinsey’s research finds 57% of organizations have a fully centralized approach towards risk and compliance when it comes to the use of AI. This is the highest level out of any AI use case, but suggests there is still potential for more haphazard approaches. Three in ten respondents say their approach is hybrid, between centralized and distributed models, while 13% rely on a fully distributed arrangement, where individual users, sites, or companies determine their own level of acceptable risk.

O’Rourke’s advice for those tasked with assessing and mitigating risk is to initially acknowledge the nature of the potential threat that arises from AI. “Embedded in this would be clear goals and framing in metrics around the AI effort,” he says. “Organizations would need to then create a governance body aligned to modifying the risks for the environment and changing the analysis of supplier evaluation, including current suppliers, who may be implementing their own AI journey.”

“This puts a burden on the procurement and risk teams of an organization to evaluate not just the largest suppliers but the broader supplier ecosystem, much like the effort for child labor, labor trafficking, sustainability, and other vulnerabilities. This should then tie in with legal to a policy statement for master service agreements, contracts, and purchase orders.”

Alongside this, organizations need to evaluate the business case for their own use of AI and to embed the governance of this in a standing risk committee, with a clear charter and leader. “Where organizations are immature or do not have a clear risk committee, then one should be formed,” he adds. “Likely members would include IT, the data analytics team, procurement, the cyber security policy leader, legal, internal audit teams, the head of risk, corporate communications, and the leader of the functions that will be implementing AI technology.”



> “
>
> Risk is about setting the right culture. Alignment, approach, and workflow is ‘check the box’ busywork to make us feel like we are productive, when in fact these activities make us less secure because it creates a false sense of protection.
>
> – Dr. Eloise Epstein
> Partner at Kearny

Use AI to Strengthen Supplier Oversight

While AI has introduced additional risks for organizations, it also has the capability to help them better control and monitor these. McKinsey's research finds 12% of businesses are already using AI in risk, legal, and compliance, and 10% do so in supply chain or inventory management. AI can extract terms from contracts, flag any expired or missing documents, map answers to policy frameworks or risk scoring logic, and help identify issues in unstructured files.

"The ability of an AI tool to screen multiple contracts in a fraction of the time of human review allows a comprehensive review of high-risk areas to further evaluate across contracts and agreements in an organization," says O'Rourke.

At Suffolk, Kociemba is using a combination of AI tools to help ensure contracts are watertight and protect the business. "The first thing I do when I get a new contract is to drop it into the Levelpath AI Assistant so I can see all the key legal obligations," she says. "If I am working with a contract that shows that a vendor has a lack of maturity, I can bring in extra resources so we can collaborate on that."

Contracts at Suffolk are automatically uploaded into Levelpath's AI-native platform, which means the organization can agentically search all of its agreements for key search terms. "It may be that we do not want to be paying late interest charges of more than 3% or that we want to make sure we have got everybody on net 60-day payment terms," she says.

The platform has also helped to end what Kociemba describes as the "chaos" of the software purchasing process, which would previously see long email threads which were almost impossible to keep track of.

"I could see we needed better safeguards around how people were purchasing," says Kociemba. "One of the issues we were running into is that if security and risk are unaware of something, they cannot evaluate it or track it. We have now established a protocol that all contracts should follow where they are routed to security and risk for evaluation so that we can more tightly control the terms." This has been welcomed by stakeholders in the business, as it provides reassurance that they are not inadvertently exposing risk into the business.

> "
>
> Levelpath allows me to scan these documents and identify who is compliant and who is not, so I can focus my energy in the right places."
>
> - Meg Kociemba,
> Senior Director
> Suffolk Construction

> "
>
> The ability of an AI tool to screen multiple contracts in a fraction of the time of human review allows a comprehensive review of high-risk areas to further evaluate across contracts and agreements in an organization,"
>
> - Jim O'Rourke,
> Award-winning Procurement
> Leader and Former CPO

The Data Dilemma

Every AI solution needs access to accurate and reliable data in order to effectively manage risk. This includes details of who suppliers are, what they access, how they access it, and which systems and data they use. However, gathering this comprehensive supplier intelligence presents a significant challenge for most organizations. Many enterprises struggle with even the basics of supplier visibility, working with tens of thousands of suppliers without anyone truly managing them or keeping a full accounting of the risks they pose.

As Dr. Epstein explained, “most ‘risk management’ occurs at onboarding, but the reality is much risk comes during operations or even offboarding.” The need to protect organizational interests throughout each supplier’s relationship lifespan makes ongoing visibility just as critical as initial checks.

From a contract perspective, accurate information around terms and obligations, including service level agreements and data processing agreements, is vital. Onboarding information is also required, including access to completed risk steps, pending reviews, history around decisions, and any mitigations that have been made.

Often, though, this information is missing, incomplete, or inaccurate. Risk data typically lives in siloed environments, controlled by different entities such as procurement, legal or information security teams, sometimes in unstructured formats that cannot be easily accessed, such as PDFs, emails, or spreadsheets. This is compounded by the fact that there is frequently no unified system of record, particularly if systems have developed over time, making it difficult to know where to find information in the first place. Most critically, the contract data that contains vital supplier terms, obligations, and risk parameters remains disconnected from operational systems, creating blind spots that can expose organizations to compliance failures, missed rebate opportunities, and supply chain disruptions.

AI can bridge these information gaps by connecting and analyzing contract data that was previously inaccessible or fragmented. The starting point when trying to get processes under control is to leverage AI to conduct comprehensive data integration and quality assurance checks, says O’Rourke. “AI can extract and connect critical contract information: payment terms, service level agreements, compliance requirements, rebate structures, and make this data actionable across the organization,” he explains. “As an example, a supplier scorecard powered by AI can automatically pull contract obligations, cross-reference them with actual performance data, and flag discrepancies that require attention, ensuring both internal alignment and supplier accountability,” he says. This connected approach transforms static contract documents into dynamic intelligence that drives better risk management, financial optimization, and operational decisions.

> “
>
> AI can extract and connect critical contract information: payment terms, service level agreements, compliance requirements, rebate structures, and make this data actionable across the organization.“
>
> – Jim O’Rourke
> Award-winning Procurement Leader and Former CPO

Modernize Third-Party Risk Management with Levelpath

New tools are emerging which are designed to help organizations better control supplier-related risk in the AI era. "Traditionally, third-party risk management has involved fragmented processes, such as questionnaires in spreadsheets, reviews over email, and siloed risk owners, making it hard to scale or provide transparency throughout the procurement process," explains Garber.

Levelpath's platform uses AI to support early risk detection by generating prompts during supplier questionnaire responses or stakeholder submissions, around issues like privacy, cybersecurity, compliance, financial health, and operational continuity.

These prompts are tailored using each company's actual third-party risk management (TPRM) policies, which remain securely contained within their proprietary Levelpath instance and are never shared outside the organization's secure environment. This ensures that critical proprietary data guides and informs the AI to empower the business without being accessible to other users or organizations. The AI can then help in assessing and interpreting responses, suggesting a preliminary risk score, and flagging any potential concerns, all while keeping the company's sensitive policies and data completely isolated and protected.

For organizations, this provides a centralized location for all third-party risk assessments, and suggests the right level of diligence to apply early on in the process. This means procurement teams can rank suppliers based on both their perceived risk and how critical their service is to the business. As risks are flagged, either through intake forms or questionnaire responses, Levelpath routes these to the appropriate teams, such as information security, privacy, legal, or compliance.

Once reviews have been completed, a structured risk record containing reviewer details, scores, and relevant documentation is created and tied to the supplier profile, which can be updated over time. Teams can also document mitigation steps within the platform and schedule reviews, create live supplier records, and flag items for follow-up. For risk teams, this creates a centralized record of supplier diligence, making accountability clear and traceable across procurement, IT, and legal stakeholders.

The Essential Knowledge For AI Risk Takers

- **How can AI improve supplier risk management:** AI identifies supplier risks earlier and gives leaders a clearer view across the supplier base.
- **How does AI support contract management:** AI reviews contracts quickly and flags compliance gaps, inconsistent terms, and hidden obligations.
- **What role does AI play in third party risk:** AI monitors supplier privacy, cybersecurity, financial health, and compliance concerns in real time.
- **How can AI strengthen procurement governance:** AI ensures that contracts, onboarding, and renewals follow organizational policies and reduce exposure.
- **Why is continuous supplier oversight important:** AI enables ongoing monitoring of suppliers and helps leaders adapt policies as risks change.

This information can then be used to factor risk into decisions such as renewals, supplier onboarding, SLAs, or expanding the use of a particular vendor. “By embedding TPRM into the broader supplier lifecycle, Levelpath helps teams move from fragmented, reactive risk reviews to proactive, policy-driven oversight that is easier to manage,” says Garber.

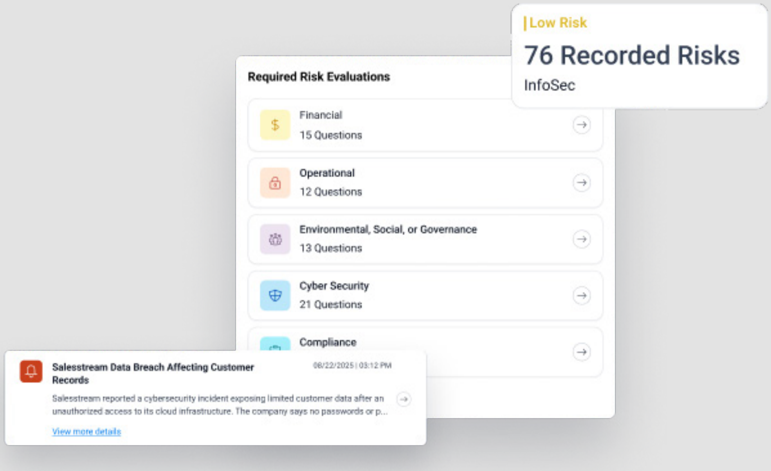
Procurement and risk teams have an important role to play in helping to transform the culture around contract and supplier management, and ensure the business remains protected in the age of AI. “Establishing that knowledge between legal, procurement, and technology teams is absolutely critical, to make sure that there is a shared understanding of what you need to protect at your organization and how you are going to do that,” says Kociemba. “We are the ringmasters coordinating with security, risk and architecture to ensure that not only are we negotiating for what we need, but what we need actually gets implemented in the contract.”

AI supplier risk management, contract management, and procurement governance are no longer optional. They are essential practices for risk, legal, compliance, and IT leaders who must ensure that supplier relationships are monitored continuously, contracts are enforced consistently, and risks are documented in a way that supports both oversight and accountability. With AI supplier oversight embedded into daily processes, organizations can move beyond fragmented reviews and toward a culture of proactive risk management that protects the business while enabling growth.

Levelpath gives risk and compliance leaders the visibility, control, and security they cannot achieve with spreadsheets or siloed tools, turning supplier oversight into a proactive, accountable process. To find out more about how Levelpath could help your business manage risk in the age of AI, visit https://www.levelpath.com/ or [book a demo]() today.

Make supplier risk management delightful.

Request a demo. ›



|Low Risk

76 Recorded Risks

InfoSec

Required Risk Evaluations

Financial
15 Questions

Operational
12 Questions

Environmental, Social, or Governance
13 Questions

Cyber Security
21 Questions

Compliance

Salesstream Data Breach Affecting Customer Records

08/22/2025 | 03:12 PM

Salesstream reported a cybersecurity incident exposing limited customer data after an unauthorized access to its cloud infrastructure. The company says no passwords or p...

View more details