The risk intelligence report

AuditBoard

Table of contents

Executive summary

Three insights define the state of risk today:

1. **AI adoption is accelerating, but trust is fragile.** More than half of enterprises are implementing AI tools and investing in skills, yet telemetry shows acceptance rates dip sharply when governance is unclear. Decision times are lengthening, confidence in AI outputs is inconsistent, and governance gaps leave many deployments stuck in pilot mode. This volatility makes AI the most visible – and most urgent – test of risk maturity today.

2. **Most enterprises are stuck in a "middle maturity trap."** Activity is high – frameworks updated, controls adopted, risks logged – but consistency is missing. Bursts of progress are followed by lapses, leaving resilience incomplete.

3. **Leaders turn governance into advantage.** They embed risk in board agendas, align teams on shared KPIs, and sustain collaboration as a discipline. The result is not just oversight, but foresight, turning risk intelligence into a driver of agility and trust.

AI is the defining test of risk maturity today. Its volatility – rapid experimentation followed by dips in acceptance – makes it the frontline dimension where ambition is highest but execution is most fragile. Enterprises are navigating a risk environment that is more complex, dynamic, and interconnected than ever before. Cybersecurity threats are intensifying, regulatory requirements are multiplying, and **the rise of the use of AI is reshaping risk at a faster pace than any other factor**. It is simultaneously the greatest opportunity and the sharpest governance challenge facing enterprises today. To keep pace, risk management must become faster, more connected, and more embedded in enterprise decision-making.

This inaugural *Risk intelligence report* offers a new benchmark for the state of enterprise risk. It draws on two complementary datasets:

1. **Proprietary AuditBoard platform telemetry**[1] (serving over 50% of the Fortune 500 and seven of the Fortune 10) from real-world activity, including AI usage, control adoption, framework mapping, collaboration, and issue logging.

2. **Survey insights**[2] from more than 400 risk leaders across North America and Europe, covering governance, maturity, and investment priorities.

[1] **Source:** AuditBoard platform telemetry, May-July 2025.

[2] **Source:** Panterra survey of 400+ risk leaders across North America and Europe, commissioned by AuditBoard (2025).

The contrast is stark. On the intent side, 53% of enterprises report implementing AI-specific tools, 39% plan to expand AI and machine learning skills, and 70% expect to increase risk management staffing over the next two years. Nearly half are updating frameworks. Yet on the behavior side, telemetry shows inconsistency:

- AI adoption surged in May and June, only to dip in July as acceptance rates fell and decision times lengthened.
- Collaboration spiked in July, then faded.
- Risk logging produced bursts of action plans, but not always backed by consistently logged risks or issues.

This volatility defines what we have described as a "middle maturity trap."[3] Two-thirds of enterprises remain siloed in structure, systems, or decision-making. They achieve activity, but not reliability. By contrast, leaders distinguish themselves through stronger alignment of people, processes, governance, and technology. They embed risk into board-level agendas, sustain collaboration through regular cadence, and treat risk logging as a discipline rather than an option.

The evidence is clear: governance, ownership, and cadence, not just investment, separate leaders from laggards. Enterprises that escape the middle maturity trap convert activity into foresight, turning risk management from reactive oversight into strategic advantage.

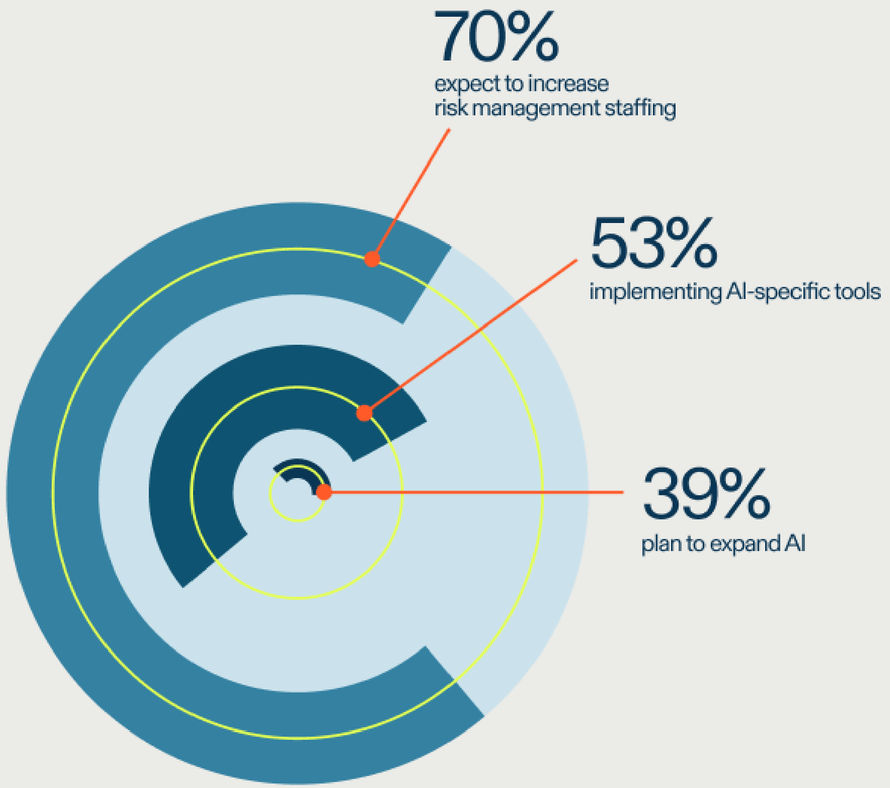
[3]**Source:** Panterra survey of 400+ risk leaders across North America and Europe, commissioned by AuditBoard (2025).

AuditBoard's platform serves:

7 of the Fortune 10

+50% of the Fortune 500

Connect risk. Connect your teams.



Introduction & context

THE CHALLENGE

Risk management today must contend with unprecedented complexity. Seven in ten risk leaders say the landscape they face is more complex than it was two years ago. New regulations, from privacy to AI governance, arrive faster than enterprises can adapt. Cyber threats evolve daily. And stakeholders such as regulators, customers, and investors expect more transparency and accountability than ever before.

> 7 in 10 risk leaders say the landscape they face is more complex than it was two years ago.

Despite this, many enterprises still manage risk in silos. Audit, risk, compliance, and information security often work in parallel, using different systems and reporting to different leaders. Without integration, their ability to provide foresight is limited.

STATE OF RISK INTELLIGENCE

Survey results reflect a market in transition. On the one hand, enterprises are investing aggressively:

- 35% are adopting new frameworks.
- 45% are updating existing frameworks.
- 39% plan to expand AI and machine learning skills.
- 40% plan to increase cybersecurity staffing.

On the other hand, maturity is lagging. Only a minority report having governance structures robust enough to embed risk intelligence across the enterprise. The disconnect between ambition and execution is stark.

THE MIDDLE MATURITY TRAP

This disconnect defines the middle maturity trap: enterprises achieve activity, but not consistent delivery. Our internal telemetry reveals the pattern. In May and June, AI adoption was strong, and in July, collaboration activity surged, but those peaks stand out precisely because they were not sustained. Our survey data shows a similar pattern of fits and starts. The volatility is evident: intent and investment are high, but governance and ownership are often lacking.

THE NEED FOR CONNECTED RISK

To break free, enterprises must adopt connected risk: integrating audit, risk, compliance, and infosec into a unified discipline. Connected risk requires shared KPIs, governance clarity, and common intelligence. It transforms risk functions from reactive monitors into strategic enablers that anticipate and shape enterprise decisions.

WHY IT MATTERS

Leaders who embrace connected risk are more resilient and more agile. They embed risk into planning cycles, ensuring new threats or regulatory demands are anticipated, not just responded to. Those who remain siloed risk slower response times, duplicated effort, and missed opportunities to leverage risk intelligence as a source of competitive differentiation.

The risk intelligence framework

True maturity is not about activity for its own sake. Logging risks, mapping frameworks, or running audits are necessary, but insufficient. What matters is whether these activities are performed consistently, at speed, and at scale. Previous research defines three key metrics to measure maturity:

1. **Level:** The scope or volume of activity.
2. **Consistency:** The reliability of those activities over time.
3. **Speed:** How quickly enterprises act once risks, controls, or insights are identified.

When we combine this research with our own proprietary dataset in aggregate, we are able to identify true measures of holistic success. Based on this holistic analysis, we have identified **five dimensions of connected risk.** Among these dimensions, AI and automation stand out as the frontline test of maturity, where ambition is highest, volatility is sharpest, and leadership is most visible.

Five dimensions of connected risk:

1. **AI & automation:** How widely and efficiently AI is used to generate, accept, and act on insights.
2. **Control maturity:** The speed and reliability of control adoption.
3. **Frameworks & coverage:** The breadth and depth of governance structures.
4. **Collaboration:** The consistency of cross-functional engagement.
5. **Risks & issues discipline:** The rigor of logging risks, tracking issues, and remediating them.

We view this framework as the gold standard for how leading enterprises actively approach connected risk. The power of this framework comes from integrating survey and telemetry data. The survey reveals intent: how leaders describe their goals and investments. The telemetry shows reality: how consistently those practices appear in day-to-day workflows. Looking at both together provides a true measure of maturity.

3 key metrics to measure maturity

Level
The scope or volume of activity.

Consistency
The reliability of those activities over time.

Speed
How quickly enterprises act once risks, controls, or insights are identified.

Dimension 1: AI & automation

Teams are using AI to draft audit narratives, accelerate control mapping, and generate insights at a speed that would have been unthinkable only a few years ago. The promise is undeniable: efficiency, foresight, and automation. **But promises alone do not equal maturity.**

Telemetry from May–July 2025 highlights this tension. In May and June, AI activity was robust: teams generated large volumes of outputs and accepted a high proportion of them, with decision times averaging just a few hours. By July, generation levels held steady, but acceptance rates fell by roughly 30%, and decision lag more than doubled. August, captured only partially, shows a steep drop in activity overall. **These snapshots reveal a clear pattern: teams are eager to experiment with AI, but their confidence in acting on those outputs fluctuates dramatically.**

Survey findings help explain the volatility in AI adoption:

- More than half of enterprises, 53%, say they are implementing AI-specific tools, and 39% are investing in AI/ML skills.
- Yet fewer than 30% feel prepared for upcoming AI governance requirements.

In many enterprises, ownership of AI oversight remains unclear, leaving enthusiasm unchecked but trust fragile. **Leaders address this gap directly.** They define decision rights, establish governance frameworks, and build internal skills to validate AI outputs, which is why their telemetry shows consistently high acceptance and shorter decision times. Laggards, by contrast, experiment actively but hesitate to commit, leaving adoption stuck in **pilot mode.**

Beyond efficiency gains, **AI and automation are redefining the audit function itself.** Teams are using generative AI to draft narratives, accelerate control mapping, and analyze evidence at scale, reducing cycle times from weeks to days. Automation not only frees auditors from repetitive tasks, but also amplifies their strategic role: surfacing anomalies earlier, linking findings to enterprise risks, and strengthening confidence in reporting. Leaders distinguish themselves by treating AI not just as a tool for speed, but **as a catalyst** for higher-quality assurance and broader organizational impact.

The lesson is clear. Enterprises that treat AI purely as an experiment will remain in pilot mode, generating outputs but struggling to depend on them. **Those that govern AI with the same rigor as other risk practices will unlock its potential and integrate it into the fabric of risk intelligence.**

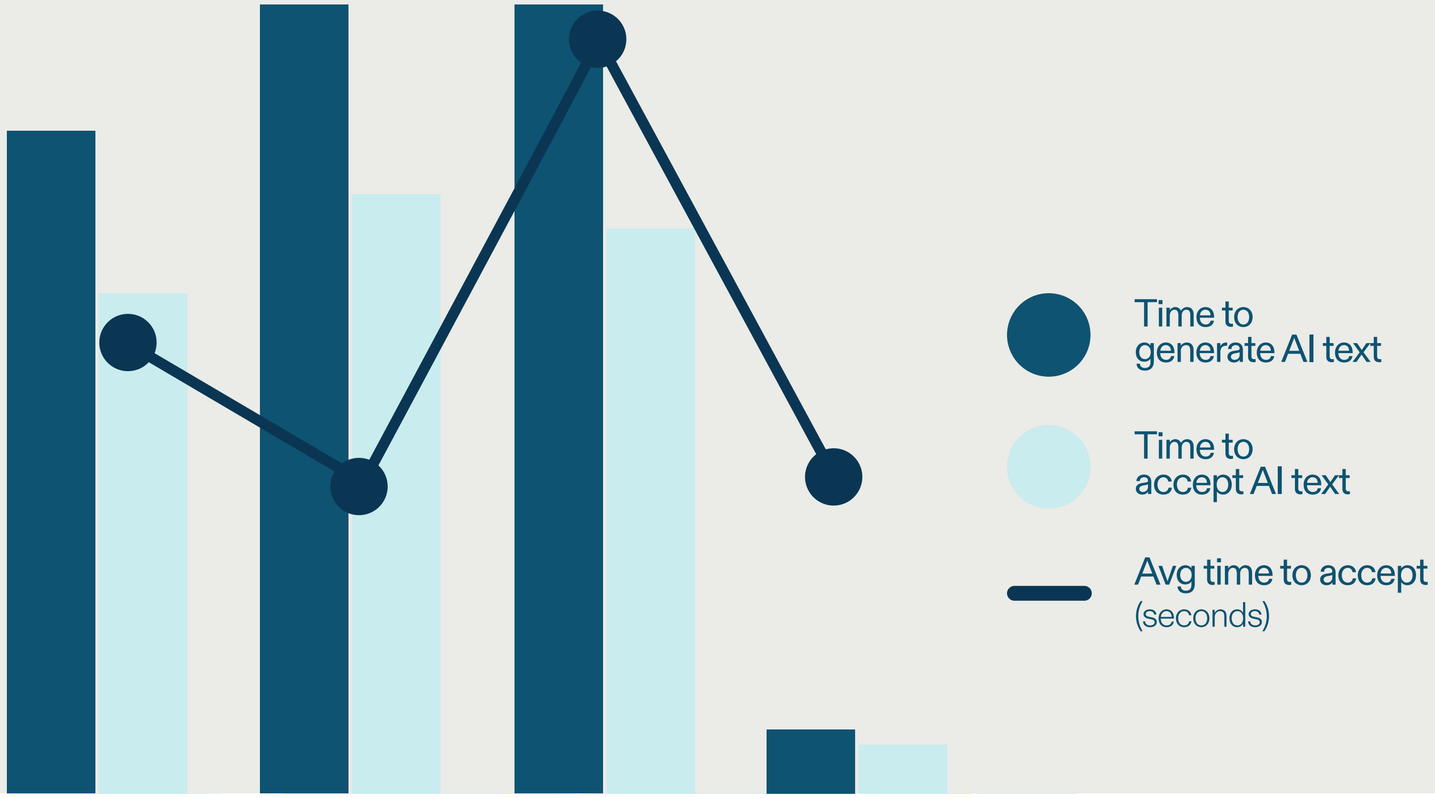
KEY TAKEAWAYS & ACTIONS

1. **AI adoption is growing, but unstable.** Telemetry shows strong experimentation followed by sharp drop-offs in confidence.
2. **Governance drives volatility.** Without clear ownership, adoption remains stuck in pilot mode.
3. **Leaders act decisively.** They assign decision rights, validate outputs, and embed AI oversight into governance.

Next step for enterprises: *Define ownership of AI governance before scaling pilots, and establish internal validation processes that build trust.*

How widely and efficiently teams use AI features

Efficiency of AI feature adoption across organizations measured by generation time, acceptance time, and average acceptance duration.



AI adoption across enterprises

Implementing

53%

Investing

39%

Preparing

30%

Dimension 2: Control maturity

Controls are the mechanisms that turn policy into practice. They define how risks are mitigated, how compliance is enforced, and how resilience is built into daily operations. **But maturity in controls is not measured by how many are documented; it is measured by how reliably they are adopted and acted upon.**

Telemetry provides a snapshot of how silos and inconsistent process delays adoption:

- In May 2025, adoption was strong: teams acted quickly on suggested controls, with guidance embedded efficiently into workflows.
- By June, response times lengthened noticeably, suggesting that bandwidth constraints or unclear ownership slowed decision-making.
- July data shows a partial recovery, with moderate adoption but still slower response times than in May.
- In August, where data is incomplete, adoption again appears to improve, though the limited coverage prevents a full picture.

Even with partial data, the signal is clear: control adoption can accelerate when governance and bandwidth are aligned, but falters when they are not.

Survey findings reinforce this story. Siloed structures, systems, and decision-making slows consistent control adoption. **Boards tend to discuss risk only reactively, and for at least 50% of enterprises, it is not a standing agenda item.** Leaders distinguish themselves by breaking this pattern. They integrate risk oversight into regular board and executive reviews, set shared KPIs across audit, risk, and compliance, and formalize adoption processes so that controls are embedded collectively rather than sporadically. Laggards, by contrast, continue to adopt controls reactively, often only in response to regulatory deadlines or audit findings.

The difference in outcomes is stark. **Enterprises that integrate control adoption into governance structures treat it as a steady discipline, making controls a consistent safeguard against emerging risks.** Those who adopt sporadically are left in cycles of last-minute compliance, exposing themselves to inefficiencies and gaps. As regulatory expectations expand, particularly around AI, cybersecurity, and ESG, the ability to adopt controls quickly and reliably will increasingly separate leaders from laggards.

The takeaway is simple: adoption speed and consistency matter as much as volume. Controls that are reviewed but not embedded provide little protection. True maturity comes when adoption is predictable, repeatable, and collective.

KEY TAKEAWAYS & ACTIONS

1. **Adoption speed matters as much as volume.** Telemetry shows adoption spikes when governance is clear, but falters when ownership is diffuse.
2. **Silos slow progress.** Many boards discuss risk reactively, leaving controls embedded sporadically rather than consistently.
3. **Leaders embed controls into governance.** They align KPIs, integrate oversight into board agendas, and adopt proactively.

Next step for enterprises: *Treat control adoption as a steady discipline by tying it to governance structures, not just compliance deadlines.*

Dimension 3: Frameworks & coverage

Frameworks are the scaffolding of risk management. They provide structure, common language, and alignment with regulatory standards. But their value depends on more than the number of frameworks adopted. What matters is depth: how thoroughly requirements are mapped and embedded into daily practice.

Telemetry offers an early view of current practice. In the months where data is available, the median enterprise maps its controls to about seven frameworks, covering roughly 2,700 requirements. Leaders go significantly further, embedding thousands more requirements into their monitoring and reporting processes. This contrast between surface breadth and true depth illustrates one of the clearest divides between enterprises moving toward maturity and those still operating at a superficial level.

Survey findings confirm that momentum is building, but depth is uneven: 35% of enterprises are adopting new frameworks, and 45% are updating existing ones. Yet many acknowledge their adoption is shallow. The result is a pattern of "surface compliance," where breadth increases but coverage is partial, leaving gaps that only surface during audits or disruptions.

Leaders treat frameworks as living systems. They selectively expand breadth while ensuring depth, mapping requirements thoroughly enough to support monitoring, reporting, and rapid response to regulatory change. Laggards adopt broadly but thinly, creating the illusion of maturity while leaving critical requirements incomplete.

This difference has significant implications. Short-term compliance can be achieved with shallow mapping, but resilience requires depth. As frameworks expand into new domains such as AI governance, ESG disclosures, and supply chain resilience, enterprises that treat frameworks as dynamic scaffolds will adapt smoothly. Those who treat them as one-off checklists will find themselves caught off guard.

The insight is clear: frameworks are not just about adoption, but also integration. Leaders measure success not by how many frameworks are in play, but by how deeply they are mapped into the fabric of operations.

KEY TAKEAWAYS & ACTIONS

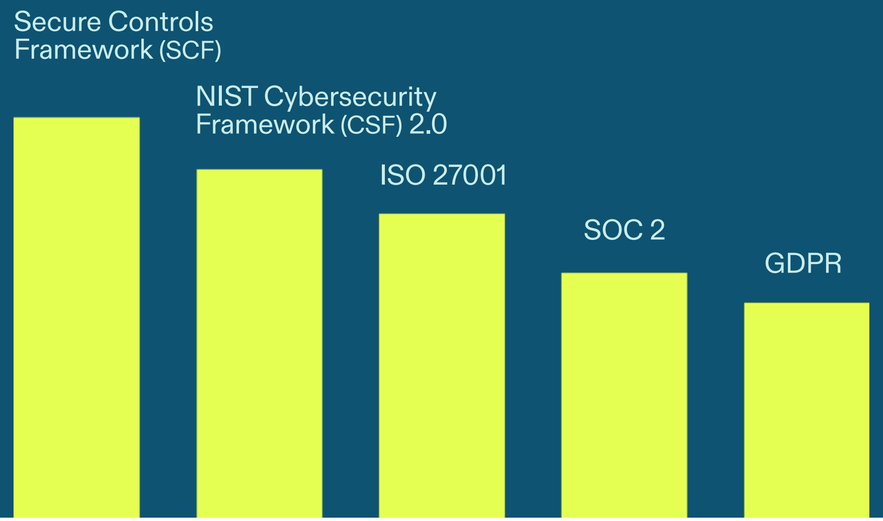
1. **Breadth is not enough.** Many enterprises adopt frameworks superficially, creating "surface compliance."
2. **Depth is the differentiator.** Leaders map requirements thoroughly into monitoring, reporting, and daily operations.
3. **Momentum is growing but uneven.** 35% are adopting new frameworks, 45% are updating, but coverage remains shallow for most.

Next step for enterprises: *Balance breadth with depth by embedding frameworks as living systems that adapt to regulatory and business change.*

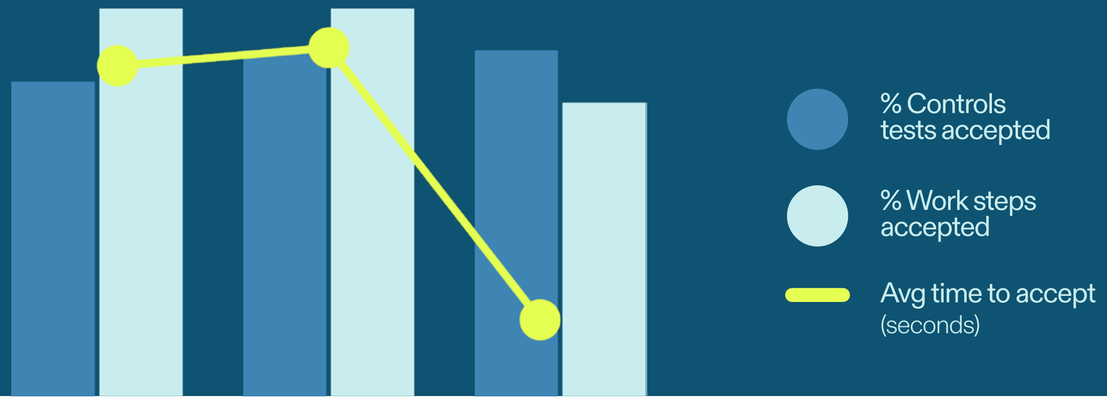
The median enterprise maps its controls to about seven frameworks, covering

~2,700 requirements

Top 5 frameworks by adoption (number of orgs)



How quickly and reliably teams act on platform guidance



Momentum is building, but depth is uneven:

35% Adopt new framework

45% Update existing framework

Dimension 4: Collaboration

Collaboration is the glue that makes connected risk possible. Audit, compliance, infosec, and the business all bring unique responsibilities, and without coordination, even the best tools or frameworks cannot deliver foresight. But collaboration is also fragile. It rises when cadence and governance are strong and fades quickly when they are not.

Telemetry provides a snapshot of this volatility. July 2025, where data is complete, shows a surge in collaboration: message volumes across Slack and Microsoft Teams spiked, and tasks advanced across functions at a rapid pace. This illustrates how cross-functional engagement can accelerate progress when supported by rhythm and structure. In other periods, where data is less complete, collaboration is harder to measure, but the absence of consistent signals highlights the same challenge that survey respondents describe: that collaboration tends to occur in bursts rather than as a steady practice.

Survey findings provide critical context. **Many enterprises remain siloed, with governance that keeps risk teams apart.** In these environments, collaboration happens only in response to external triggers, such as an audit cycle or regulatory demand. Leaders, by contrast, make collaboration part of the operating model. They hold regular cross-functional risk meetings, align teams on shared KPIs, and institutionalize coordination through predictable routines.

The outcomes diverge clearly. **Leaders surface risks earlier and resolve them more consistently because collaboration is embedded.** Others experience spikes of activity followed by long gaps, leading to slower responses and duplicated effort. As AI governance and ESG requirements gain traction, the need for seamless coordination across teams will only grow. Enterprises that embed collaboration into governance structures today will be positioned to respond with agility tomorrow.

KEY TAKEAWAYS & ACTIONS

1. **Collaboration is fragile.** Telemetry shows bursts of cross-functional activity, but little consistency over time.
2. **Silos create stop-and-go engagement.** Many risk teams only coordinate in response to audits or regulatory demands.
3. **Leaders institutionalize collaboration.** They set shared KPIs, hold regular cross-functional meetings, and build predictable routines.

Next step for enterprises: *Make collaboration a part of the operating model by embedding it into governance cadence, not leaving it to chance.*

Dimension 5: Risks & issues discipline

Capturing risks, surfacing issues, and developing remediation plans are the backbone of mature risk management. Without reliable processes for logging exposures and tracking follow-up, enterprises cannot build the foresight required to anticipate threats or measure progress.

Telemetry offers a glimpse of how uneven this discipline can be. In the periods with stronger coverage, action plans were created at meaningful volume, but often without corresponding risks or issues logged beforehand. This disconnect suggests that remediation is not always tied to a clear record of exposures, a sign of ad hoc rather than systematic practice. Peaks in activity show that teams can capture and address risks effectively, but gaps in the data mirror gaps in behavior: logging is not yet a consistent habit.

Survey findings sharpen the contrast between leaders and laggards. Enterprises conducting six or more risk assessments per year report stronger overall risk discipline. They know risk capture shouldn't just be periodic, but ongoing and automated where possible. They are also more likely to have increased assessment frequency over the last two years. By contrast, the median enterprise conducts far fewer assessments, often reacting to external triggers rather than maintaining steady evaluation. Silos in structure or decision-making compound the problem by scattering accountability for risk capture across functions.

The difference in outcomes is stark. Leaders who institutionalize assessment cadence and embed it into governance routines demonstrate higher telemetry scores for logging and remediation. They ensure risks are identified, issues are tracked, and action plans are reliably executed. Laggards, by contrast, see peaks of activity followed by silence – evidence that risks are logged only when urgent, leaving exposures invisible until problems escalate.

The lesson is clear: what gets logged gets managed. Until enterprises treat risk and issue capture as a regular management habit, they will remain stuck in cycles of reaction, with remediation divorced from visibility.

KEY TAKEAWAYS & ACTIONS

1. **Logging gaps weaken resilience.** Telemetry shows action plans often created without corresponding risks logged, evidence of ad hoc practices.
2. **Cadence drives maturity.** Enterprises conducting six or more assessments per year report stronger discipline and telemetry scores.
3. **Continuous monitoring closes the loop.** Leaders go beyond periodic assessments by embedding monitoring into workflows, ensuring exposures surface in real time.
4. **Leaders build habits.** They institutionalize logging and remediation so nothing remains hidden.

Next step for enterprises: *Treat risk capture as a management habit. What gets logged gets managed. Establish continuous monitoring alongside regular assessments to ensure risks are visible and acted on consistently.*

Strategic roadmap for enterprises

The five dimensions of risk intelligence – AI and automation, control maturity, frameworks and coverage, collaboration, and risks and issues discipline – reveal both progress and inconsistency. Enterprises are moving forward, but often in bursts that fade. To escape the middle maturity trap, leaders need a structured roadmap that connects intent with execution.

We see this journey unfolding in three phases.

Phase 1: Establish governance clarity

- Define ownership and accountability through enterprise risk committees.
- Make risk oversight a standing item at board and executive meetings.
- Align structures to eliminate silos across audit, risk, compliance, and infosec.

Phase 2: Drive execution discipline

- Set shared KPIs across functions to sustain adoption speed and consistency.
- Institutionalize regular cross-functional meetings.
- Make assessment cadence non-negotiable, supported by continuous monitoring.

Phase 3: Scale market leadership

- Balance breadth and depth in framework adoption, ensuring resilience rather than surface compliance.
- Scale AI responsibly. Embed AI into daily workflows with validation and governance so it becomes a trusted enabler, not an unchecked experiment.
- Treat risk not as a compliance overhead, but as a driver of foresight, resilience, and competitive advantage.

A maturity journey, not a checklist

The roadmap is not a linear list of actions. It is a maturity journey. Each phase builds the capacity for the next. Governance enables execution. Execution creates the reliability needed for strategy. Leaders who follow this path move beyond sporadic progress and create a system of risk intelligence that is connected, repeatable, and strategic.

This journey unfolds in three phases.

Phase 01

ESTABLISH GOVERNANCE CLARITY

Phase 02

DRIVE EXECUTION DISCIPLINE

Phase 03

SCALE MARKET LEADERSHIP

Conclusion

The story that emerges from this report is both encouraging and cautionary. Enterprises are moving forward. They are investing in AI tools, expanding their frameworks, hiring for new skills, and building risk functions that are more visible than ever before. Yet, telemetry reminds us that **intent is not the same as execution.** Even as enterprises generate large volumes of AI outputs or log risks in bursts, adoption often falters, collaboration fades, and consistency breaks down.

Most enterprises are stuck in the **middle maturity trap:** bursts of progress without sustained reliability. Leaders, however, show what's possible by embedding discipline into every dimension of risk intelligence.

Leaders distinguish themselves by:

- **Turning AI from experiment to trusted partner** – embedding governance, defining ownership, and validating outputs.
- **Adopting controls consistently and quickly** – enabled by clear governance and shared KPIs.
- **Balancing breadth and depth in frameworks** – treating them as living systems, not one-off checklists.
- **Designing collaboration into processes** – sustaining cross-functional engagement through regular cadence.
- **Making risk logging a discipline** – ensuring exposures are visible, monitored continuously, and tied to remediation.

These practices are not isolated. Together, they form a system of risk intelligence: **connected, repeatable, and embedded in strategy.** That is why leaders can move faster, anticipate change, and rarely find themselves caught off guard.

The path ahead is clear. Enterprises that treat risk intelligence as an integrated system rather than a series of siloed improvements will move beyond the middle maturity trap. They will not only keep pace with complexity but will turn risk management into a source of foresight and advantage. Those who hesitate will remain fragmented, experiencing progress in bursts but never reaching the maturity needed to thrive.

The choice is not whether to act. It is whether to build a system that endures.

How leaders distinguish themselves

- Turning AI from experiment to trusted partner
- Making risk logging a discipline
- Adopting controls consistently and quickly
- Designing collaboration into processes
- Balancing breadth and depth in frameworks

Appendix

RESEARCH METHODOLOGY

The survey included 432 respondents sourced from a leading global online panel provider. They were selected from the panel based on geographic and role-based quotas, as well as screening questions based on role in audit and compliance, decision-making role, company size, and how long they have been in their audit role. All participants were Audit, GRC, or IT decision-makers and purchase influencers working at companies with annual revenue of at least $100 million USD. Selected respondents were further screened based on self-reported audit and compliance knowledge and attentiveness to survey questions.

ROLE QUOTAS

The survey divided respondents into four broad roles: C-suite 50%, Lead 45%, Manager 5%. Respondents were asked to select which role – from a list of 23 options – most closely described their primary responsibility, even if none were quite right or even if they performed more than one of these roles. Answers were consolidated into those four broad roles.

GEOGRAPHIC QUOTAS

The survey included respondents from the U.S., Canada, Germany, and the UK.

INDUSTRY

Although no industry-level quotas were deployed, we monitored the data to ensure that no single industry was overrepresented in the data. The final breakdown of respondents by industry is as follows: Financial Services 17%, Retail / Ecommerce 10%, Industrial and Manufacturing 12%, Energy & Resources 17%, Transportation and Logistics (including supply chain) 4%, Life Sciences (including healthcare and pharmaceuticals) 3%, Insurance 10%, Technology 4%, Business / Professional Services 3%, Education 5%, Government / Public Sector 2%, Telecommunications 8%, and Marketing and Advertising 5%.

RESPONDENT SCREENS

Role: All respondents were required to indicate that they were responsible for or had influence in evaluating and/or selecting audit compliance solutions or software for their organization.

Company size: All respondents must self-report that their companies have a minimum of 250 employees. All potential respondents from smaller companies were excluded. In total, the survey includes 16% of respondents from companies with 250-499 employees, 33% from companies with 500-999 employees, 28% from companies with 1,000 to 4,999 employees, 12% from companies with 5,000 to 9,999 employees, 5% from companies with 10,000 to 24,999 employees, 1% from companies with 25,000 to 49,999 employees, and 6% from companies with 50,000 or more employees.

Time in IT: Respondents must have spent a minimum of 3 years managing, planning, or purchasing compliance and/or cyber risk management software services or infrastructure in order to qualify for the survey. In total, 20% of respondents have spent 3 to 5 years in this role, 55% have spent 6 to 10 years in this role, 20% have spent 11 to 15 years in this role, and 5% have spent 16 years or more in this role.

Information level: In our experience, it is possible to have "qualifying respondents" who nevertheless prove to have too little information or knowledge about the space to provide useful data from which to draw insights. We therefore apply an "information" screen to respondents as well. Specifically, we ask whether or not respondents could explain certain terms to their colleagues if asked to do so. In order to qualify for this survey, a respondent must say "yes" to this question for the term "GRC (Governance, Risk, and Compliance)"

"Attention" level: It is easy for respondents to speed through surveys or not pay enough attention to provide useful data. We make an effort to exclude these respondents as well, as they provide generally less useful data. In this survey, respondents were screened out for "attention" reasons if they said they could explain the made-up term "CRISM Framework" to a colleague in the same question used for the Information Screen noted above.

RESPONDENT SCREENS

It is technically impossible and improper to list a margin of error for a survey of this type. The respondents for this sample were drawn from an online panel with an unknown relationship to the total universe, about which we also do not know the true demographics. As such, the exact representativeness of this, or any similarly produced sample, is unknown.