Optro

Human behavior

The AI risk surface GRC can't ignore



Table of contents

Intro — 03

The AI visibility gap — 04

The AI accountability gap — 05

What good GRC AI governance looks like — 06

The future of GRC AI governance — 08

About Optro — 09

Appendix — 10

Introduction

The right AI governance strategy is critical to safely and securely harness the technology's power.

Most organizations are worried about AI technology itself, particularly how the models underpinning these tools can go haywire, leading to hallucinations, adversarial attacks, bias, and frontier capabilities. These unintended outcomes can and do occur, but this framing misses an important element: that the greatest risk of AI misuse actually stems from human actions.

Recent survey insights from over 800 IT, security, audit, and governance, risk, and compliance (GRC) professionals confirm that the more immediate and less-explored risk surface involves employees using AI every day, often without oversight, inside tools that were never formally vetted or approved. Behavioral risk, the decisions employees make with AI tools, is both more urgent and less governed than technical model risk. Organizations can only solve this challenge with the right AI governance strategy, which not only puts the right behavioral guardrails in place, but also advocates for continued human-in-the-loop involvement.



The AI visibility gap

The visibility gap is the core barrier to establishing effective AI governance. And the problem is worse than most realize:

- Only 34% of organizations have an AI model inventory
- Only 31% have AI incident response procedures
- Only 18% auto-block unauthorized AI domains

You cannot monitor, govern, or respond to what you haven't cataloged. Part of this challenge is what employees even consider "using AI."

More than half (56%) of organizations already use embedded AI in vendor tools. This is nearly as prevalent as generative AI (63%), but far less visible. Employees don't always think of embedded AI as "using AI" — they think of it as using their contract management tool, their email client, or their audit platform. But the reality is that these tools heighten the potential for third-party threats.

- 44% say they are concerned about employees' lack of awareness of AI embedded in tools (55% among C-level).
- 64% of audit, GRC, or IT decision-makers and purchase influencers only feel somewhat confident to somewhat unconfident about their organization's visibility into third-party cyber risk, including risks posed by vendor AI capabilities.
- Chief information security officers (CISOs) are significantly less confident than their peers regarding the risks closest to them: they lag the broader sample by 22% on third-party cyber risk visibility, and by 11% on their organization's ability to respond to an AI-enabled incident without internal friction.

The top behavioral concerns among GRC leaders are employees inputting confidential business data into AI tools (62%) and exposure of personally identifiable information (PII) or customer data (62%). Shadow AI — or employees using unapproved tools — concerns 59%, while relying on AI without verification worries 60%. These aren't rare scenarios. They're daily behavior patterns happening right now, across every function, in tools often invisible to governance teams.

These results show that employees use third-party AI tools in ways and places completely ungoverned by GRC, but also that security professionals might not even feel properly deputized to address AI risks and incidents when they occur. And this is directly leading to a significant uptick in AI-enabled attacks:

- 82% reported an increase over the past year, with 39% reporting a significant increase.
- For CISOs specifically, 72% say attacks have significantly increased.
- Social engineering is the top threat priority, ahead of ransomware, and 61% say it has increased compared to last year.

AI isn't a future threat; it's an active, escalating one. And the primary attack vector isn't technical exploitation of AI models. It's humans being manipulated by AI.

The reality	The problem
ONLY **34%** of organizations have an AI model inventory	**82%** report an increase in AI-enabled attacks over the past year

The AI accountability gap

Determining who is responsible for the risks these tools generate poses another challenge. If GRC professionals can't govern what they can't see, they also can't govern what they don't even know they're responsible for. And most survey respondents are, indeed, concerned about gaps in AI governance, and worry that permissive policies will make AI-driven attacks even worse:

- 35% of respondents (40% of CISOs) believe that if AI governance policies are too permissive, AI-enabled social engineering and impersonation will increase.
- 30% overall, and 42% of CISOs say their primary concern about the future policy environment is insufficient focus on AI governance and emerging threats.

The worry isn't that AI will become dangerous in the abstract. The worry is that weak governance creates the conditions where human behavior becomes the exploit. Yet, that is the reality for a third of organizations surveyed, who said they feel responsible for risks they can't actually control. For CISOs specifically, a third say accountability and authority are misaligned with third-party AI risk. If an AI-enabled security incident escalated quickly, the majority, at 69%, said they were only somewhat confident to not very confident that their organization could respond decisively without internal friction, including department silos and unclear decision-making.

The data doesn't point to one dominant resource or capability gap that most limits security leaders' ability to address AI-driven cybersecurity concerns, but looking at subgroups reveals that:

- 23% of CISOs say a lack of personnel with expertise in AI security or emerging risks is the biggest blocker, while 22% say clear accountability frameworks that match controls.
- 31% of internal audit respondents also cite a lack of personnel with expertise in AI security or in emerging risks.
- 23% of compliance professionals say they don't have the tools for continuous monitoring of supply chain risk, while 21% say clear accountability frameworks that align with controls do not exist.
- 25% of IT security professionals blame a lack of budget to address AI-driven and evolving threats.

From these responses, it is worthwhile to call out the apparent talent gap hampering certain AI security activities. This means organizations face an accelerating threat pattern without the people who know how to read it. This isn't just a governance design problem. When accountability is unclear or organizations lack the skills to address threats, behavioral risks go unaddressed because no one owns the response.

30% overall, and 42% of CISOs

say their primary concern about the future policy environment is insufficient focus on AI governance and emerging threats.



What good GRC AI governance looks like

If you take the insights from the visibility and accountability gaps together, a common theme emerges. Silos — employees' individual, uncovered usage of AI and GRC professionals' lack of understanding of which team owns what — presents perhaps the biggest barrier to effective AI governance. Silos breed inconsistency, lack of transparency, and inability to respond to AI-driven threats.

Our survey found that organizations with high cross-functional integration of AI processes and procedures throughout the business report better outcomes in nearly every area. Much of this approach comes down to organizational design. When organizations embed the right processes and guardrails for AI use across teams, with proper accountability and authority established across GRC and other related teams, they get closer to using AI safely and successfully. Some of the benefits of cross-functional integration cited in the survey insights include:

- Faster risk identification: 58%
- Better regulatory readiness: 54%
- Improved executive reporting: 52%
- Improved remediation prioritization: 52%
- Reduced duplication of effort: 44%
- Reduced audit fatigue: 36%

If we look more closely at the respondents who specifically say they have high cross-functional integration compared to low, these benefits increase:

BENEFIT	HIGH INTEGRATION	LOW INTEGRATION
Faster risk identification	61%	54%
Better regulatory readiness	56%	44%
Improved remediation prioritization	56%	50%
Improved executive reporting	58%	40%
Reduced duplication of effort	45%	35%
Reduced audit fatigue	41%	35%

Achieving this cross-functional integration requires both bringing together teams to streamline processes and communication around AI usage and using the right technology to establish the right controls and monitor risk.

People

From a people perspective, bringing together a management-level committee can better formalize how to approach developing and executing AI across the organization together. This approach creates a collaborative network where different teams can share insights and identify potential blind spots. This governance committee should involve legal, compliance, IT, data science, and the specific business units using the AI tools. An approach like this helps delineate each team's roles and responsibilities for proper AI governance.

TEAM	RESPONSIBILITY
The board	Sits at the forefront of this group to champion the AI strategy
Finance	Defines tracking of key performance indicators (KPIs) where AI can make the biggest impact and drive the greatest efficiencies
Legal	Assesses regulatory risks
Data science	Evaluates model performance
IT	Operationalizes AI to enable understanding of the processes and tools in use, as well as checks for both their inputs and outputs
Audit	Demonstrates how to achieve security in these new processes, and identifies within AI models where human intervention is necessary
Human resources	Considers the impact on employees

This cross-functional collaboration ensures that your governance strategy is comprehensive, practical, and aligned with the realities of your business operations, building a more resilient and responsible AI ecosystem.

Technology

As your organization adopts more AI tools, manual oversight becomes impossible. You can't rely on spreadsheets and email chains to manage the complex risks associated with dozens or even hundreds of models. Using integrated technology to automate governance — yes, including AI within the platform itself — turns policy into practice.

AI governance platforms provide a centralized system to enforce your policies consistently across all internal and third-party AI tools. The right platform can help you operationalize your framework by automating critical tasks like bias detection, risk assessments, and compliance monitoring. The best platform will allow for:

- **Centralized AI intake and tracking** that automates manual governance activities and reduces risk by bringing all AI model intake, reviews, and approvals into one place
- **Streamlined, unified AI compliance** that lets you meet evolving AI standards while connecting models to relevant policies, risks, and controls to strengthen your security posture
- **Continuous risk monitoring** that helps unify your AI risks and move beyond manual tracking with intelligent risk scoring, suggested control mappings, and actionable mitigation steps

By using integrated technology to automate governance, you can achieve shared visibility into AI usage, more urgent, unified incident response, and clear ownership of behavioral risk.

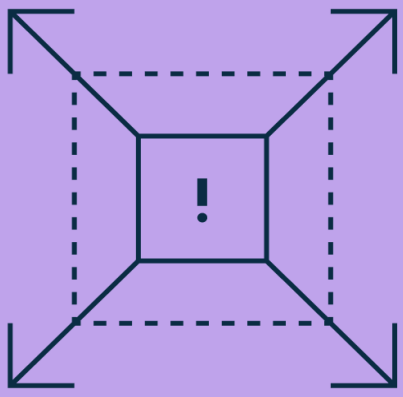
The future of GRC AI governance

The very same causes of AI risk — technology and the people using it — are also the solutions to preventing it. Technology use without process and parameters can cause both intended and unintended consequences. Your employees need adaptable AI governance frameworks to follow, and a robust, connected platform to activate, modify, and manage these guidelines. These guardrails can elevate GRC as a proactive, rather than reactive, resource for enabling responsible, scalable AI-driven innovation and productivity.

About Optro

Optro (formerly AuditBoard) helps enterprises transform risk into opportunity, redefining GRC through an agentic system of action. More than 50% of the Fortune 500 trust Optro to elevate audit, risk, and compliance in addressing a new era of risk. Optro is top-rated by customers on G2 and was named a Leader in the 2025 Gartner® Magic Quadrant™ for Governance, Risk and Compliance (GRC) Tools, Assurance Leaders. To learn more, visit: optro.ai or get in touch with our team today.





Appendix

RESEARCH METHODOLOGY

The survey included 822 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 26%, Lead 57%, Manager 16%. Respondents were asked to select which role – from a list of 31 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 11%, Industrial and Manufacturing 10%, Energy & Resources 5%, Transportation and Logistics (including supply chain) 2%, Life Sciences (including healthcare and pharmaceuticals) 8%, Insurance 8%, Technology 18%, Business / Professional Services 6%, Education 2%, Government / Public Sector 5%, Telecommunications 7%, Nonprofit 2%, and Marketing and Advertising 1%.

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 6% of respondents from companies with 250-499 employees, 20% from companies with 500-999 employees, 40% from companies with 1,000 to 4,999 employees, 18% from companies with 5,000 to 9,999 employees, 6% from companies with 10,000 to 24,999 employees, 3% from companies with 25,000 to 49,999 employees, and 7% 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, 29% of respondents have spent 3 to 5 years in this role, 49% have spent 6 to 10 years in this role, 18% have spent 11 to 15 years in this role, and 4% 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.

MARGIN OF ERROR

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.