SAI360
RISK FROM EVERY ANGLE

2026 GRC, Ethics & Compliance Guide

Trends You Need to Stay Ahead

Table of Contents

Introduction

In 2025, the balance between risk and reward became materially more consequential.

Breakthroughs in AI, rising expectations for operational resilience, and intensifying regulatory scrutiny are reshaping executive agendas. Seizing technological opportunities while managing interconnected, multi-layered risks is a defining capability differentiating market leaders from those constrained by reactive risk management.

GRC, ethics, and learning are genuine competitive differentiators in this context; disciplines that actively create value by equipping leaders with the clarity, structure, and guardrails to thrive amidst volatility.

Fulfilling that mandate requires a grounded view of risk and compliance trends and, where possible, meaningful foresight into what comes next.

This eBook explores the key themes that shaped 2025, what they mean for GRC professionals, and how you can prepare to deliver value in 2026.

The commentary within this paper is based on our recent webinar 2026 GRC, Ethics & Compliance Guide: Trends You Need to Stay Ahead. Topics include:

- **Artificial Intelligence:** expanding opportunity and evolving risk
- **Integrated Risk Management:** what it is and why it matters now
- **Geopolitical and Regulatory Uncertainty:** navigating the new landscape

Artificial Intelligence: Opportunities and Risks

Generative AI (GenAI) continues to dominate strategic conversations, both among leaders eager to deploy it and GRC practitioners responsible for doing so safely. In 2025, we saw a decisive shift from experimentation to operationalization, fueled by improvements in model performance and clearer business use cases. Enterprises have already invested tens of billions into GenAI, and there are no signs of slowing.[1]

The GRC Mandate: Assuring AI Without Stifling Innovation

As the benefits of GenAI begin to materialize – unevenly but visibly – adoption accelerates, expectations rise, and competitive pressure intensifies. Today, 79% of leaders believe they need to adopt GenAI to remain competitive.[2]

Yet organizations are still hampered by immature governance frameworks, unclear accountability, and assurance processes not built for AI. Many firms are spending 30–50% of their GenAI innovation time on compliance work, slowing delivery and eroding ROI.[3]

Meanwhile:

- Only 18% of firms have an enterprise-wide Responsible AI council,
- a third require risk awareness or mitigation skills for technical staff, and
- fewer than a quarter embed risk mitigation directly into their development processes.

Move too slowly and the business case evaporates. Move too quickly and risk exposure spikes. The goal is to provide assurance without constraining innovation.

1. https://mlq.ai/media/quarterly_decks/v0.1_State_of_AI_in_Business_2025_Report.pdf
2. https://www.microsoft.com/en-us/worklab/work-trend-index/ai-at-work-is-here-now-comes-the-hard-part
3. https://www.mckinsey.com/capabilities/tech-and-ai/our-insights/overcoming-two-issues-that-are-sinking-gen-ai-programs

The Expanding GenAI Risk Landscape

GenAI has dramatically broadened the risk perimeter. What once centered on bias and robustness now includes cybersecurity threats, hallucinations and inaccuracy, regulatory exposure, privacy concerns, intellectual property risks, and even geopolitical and national security implications.[4]

To gauge where practitioners feel the most pressure, we asked webinar attendees (n = 74):

"Which GenAI risk presents the most pressing governance challenge for your organization right now?"

Risk	Response rate
Cybersecurity	36.49%
Inaccuracy	29.73%
Regulatory Compliance	20.27%
Personal / Individual Privacy	9.46%
Intellectual Property Infringement	4.05%

Cybersecurity and inaccuracy dominate GRC and ethics concerns, with regulatory compliance close behind. GenAI risks cut across both operational and compliance domains.

COMPLIANCE RISK WILL CONTINUE TO INTENSIFY

Regulators police outcomes. As AI increasingly shapes those outcomes, it becomes regulated from every direction, explicitly through AI-specific rules and implicitly through every existing compliance regime it touches.

DIRECT REGULATION

Purpose-built AI frameworks, such as the EU AI Act, introduce specific obligations for design, deployment, monitoring, and documentation.

INDIRECT REGULATION

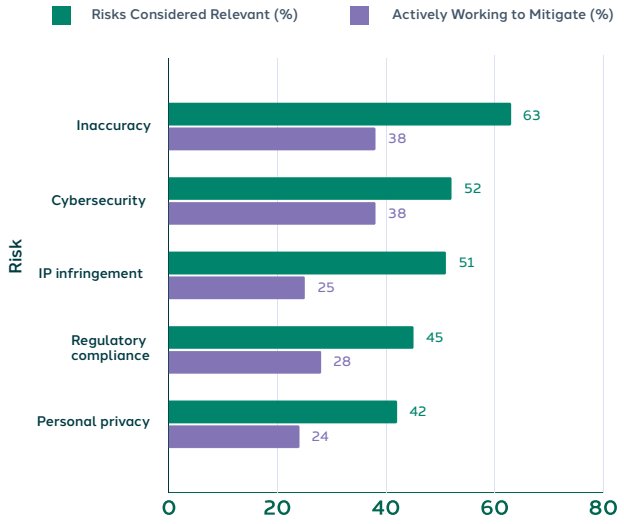
Existing laws not written for AI (GDPR, NIS2, DORA, CPRA) still apply fully to AI-enabled processes. As AI becomes embedded in decision-making, these obligations become more complex and more consequential.

The challenge for organizations is maintaining visibility, readiness, and control in an environment where AI innovation outpaces regulatory interpretation.

The Gap Between Knowing and Doing

Most organizations recognize the breadth of GenAI risks, and many have already experienced real consequences. In recent McKinsey research, 44% of respondents reported at least one negative outcome from the use of GenAI.[5]

Yet far fewer organizations are actively mitigating the risks they consider relevant. Awareness is high, but action lags, widening the governance gap as AI adoption accelerates.



- Chart created from McKinsey Data

4. https://henko-ai.com/wp-content/uploads/2024/09/the-state-of-ai-in-early-2024.pdf
5. https://henko-ai.com/wp-content/uploads/2024/09/the-state-of-ai-in-early-2024.pdf

Closing the Gap

Leading organizations clearly define how AI will and will not be used. This is fundamentally about policy; the foundation on which everything else rests. While organizations must meet external regulatory requirements, leading firms go further by anchoring their AI policies in their own risk appetite and values. These are conscious choices that need to be documented.

1. Clear Policies and Boundaries

Firms with clear, well-communicated policies moved faster and safer than those with advanced tooling but unclear rules.

2. Shared Accountability Across the Lifecycle

The golden question is: *who is responsible for GenAI?* **And the answer is:** *everyone.*

AI governance works best when ownership is distributed. Because GenAI has such wide-ranging implications, you can't confine governance to a narrow circle of data scientists and risk managers. Legal, compliance, IT, HR, and marketing all need a seat at the table.

3. Training for a New Reality

Annual, generic training is no longer fit for purpose. High performers began shifting towards:

- Role-specific, context-driven learning
- Continuous micro-training rather than once-a-year modules
- Education focused on distinguishing enterprise-approved tools from public AI systems

This approach better reflects how employees actually encounter and use AI in their day-to-day work.

4. Visibility and Control

Catalogue all AI models and systems – those you built and those you procured – in a centralized model inventory. Be clear whether you are acting as a provider or a deployer under regulations like the EU AI Act.

For each system, clearly define the use case: what exactly does the AI do, and where does it sit within the workflow? Be granular. Saying "We use GenAI for customer service" is not enough; does it support frontline interactions, produce summaries, or handle escalations? That level of detail matters.

A robust inventory should include all machine-learning repositories, contracts or subscriptions for third-party AI services. Input from department leads may be required to surface any shadow AI usage.

2026: Moving Beyond "What Is the Risk?" to "What Are the Controls?"

If 2025 was the year organizations built foundations, 2026 will be the year they operationalize them. The conversation is shifting from *"What's the risk?"* to *"Are our controls working, repeatable, and scalable?"*

When it comes to AI risk, the fundamentals don't change just because the technology does. A risk assessment is still about asking the same core questions: what new risks are emerging, how severe are they, and can we make them more predictable and controllable?

That means building on the frameworks we already have — operational risk, compliance, cyber — and applying them to AI. The lens might be new, but the scaffolding is familiar.

Evaluating GenAI Risk

Every AI system should be assessed against a handful of essential qualities:

- Is it **safe?**
- Is it **secure and resilient?**
- Is it **explainable and interpretable?**
- Is it **privacy-enhanced?**
- Is it **fair and unbiased?**

And underpinning all of this: is it **valid and reliable?**

When a system falls short in any dimension, the key question is: *What is the impact on customers, regulators, society, or the business?* This approach will shape the control environment.

2026 will not be action through manual effort. It will be action through technology. Organizations will increasingly fight fire with fire, using AI to govern AI. Across our work with customers and industry leaders, several AI-enabled use cases consistently stand out as the most transformative for risk and compliance:

- **Risk identification and forecasting** through anomaly detection and predictive analytics.
- **Personalized, continuous training** aligned to individual behavior and role.
- **More intelligent whistleblowing workflows** with automated form generation and routing.
- **GenAI-enabled text analysis:** horizon scanning, gap analysis, policy drafting, audit support, and comms monitoring.
- **External risk intelligence** that detects emerging threats in real time.
- **Investigative co-pilots** that reason over enterprise knowledge to guide decision-making.

For a deeper dive into these use cases, including practical examples, data, and how organizations are already deploying them, check out our paper: How AI is Rewriting the Compliance Playbook

The Mandate for Integrated Risk Management

2025 reinforced the imperative to understand and manage the cumulative impact of risks.

Operating models are becoming increasingly technology-dependent and decentralized, and third parties are handling a greater operational load. This shift is deepening dependencies across systems, people, and processes, making risks more tightly coupled.

Cyber, climate, supply-chain, human capital, and geopolitical risks are each material in their own right. Taken together, however, they create nonlinear and compounding exposures that are significantly harder to anticipate, assess, or model.

We asked webinar attendees to identify the top five risks they expect their organizations to face over the next three years.

What are the top 5 risks your organization faces in the next three years? (n = 48)

Risk	Response rate
Cybersecurity and data security	37.5%
Business continuity and operational resilience	37.5%
Digital disruption (including AI)	12.5%
Human capital and talent management	12.5%

This distribution is broad but familiar, capturing the diversity of risks that GRC, ethics and learning need to consider. Ranking is an essential mechanism for prioritization, but the more meaningful insight lies in the relationships between these risks rather than the rankings themselves. Cybersecurity threats directly undermine operational resilience; digital disruption reshapes talent requirements; and geopolitical tensions exacerbate supply-chain fragility. No single risk exists in isolation.

Integrated risk management is the response to this reality. It requires organizations to look beyond silos, examine where risks converge, and prepare for cascading-disruption scenarios. It has been a key goal for organizations throughout 2025, and will only grow more important in 2026 and beyond.

Outages in 2025

Major outages occurred monthly, sometimes weekly. The causes are becoming more diverse, the impacts more widely felt, and the repercussions and forensic details more widely scrutinized. Recent case studies illustrate how localized failures can be amplified as disruptions spread across interconnected systems and processes, with the cumulative impact almost always exceeding the original trigger.

Example	Causal Chain / Cumulative Impact
CME Group Futures Outage (Nov 2025)	A cooling plant malfunction at a CyrusOne-operated data center in Chicago knocked out multiple chillers, causing temperatures to rise rapidly and triggering a prolonged systems failure. Under CME Group's recovery plan, operations should have failed over to a secondary data center in New York. However, early internal and external communications suggested the issue would be short-lived. This lack of clarity delayed decisive failover actions and prolonged exposure. The combination of factors ultimately cascaded into an 11-hour global outage of the CME Globex trading platform.
Cyberattack on Marks & Spencer (April 2025)	Attackers gained access via a third party by calling the service desk and persuading staff to reset a password. The initial ransomware attack evolved into: • **Technology risk:** Core systems were taken offline to contain the breach. • **Operational risk:** Stores were unable to process payments or manage inventory. • **Supply-chain disruption:** Logistics and stock management systems failed, and additional IT infrastructure was shut down as a precaution, leading to empty shelves. • **Financial impact:** Profit before tax fell by 99%.[6]

6. https://www.bbc.com/news/articles/c93x16zkl9do

These are just two examples drawn from a much broader pattern of disruption in 2025.

Similar incidents include multiple banking outages in the United Kingdom, affecting institutions such as Barclays and Lloyds; a fire at an electrical substation in Hayes, London, which caused a complete power outage at Heathrow Airport; a major AWS outage that effectively brought large parts of the digital economy to a standstill; and even so-called "world firsts" – the widespread power outages across Portugal and Spain.

In every case, the distinction between technical and physical risk is irrelevant to customers, regulators, and the bottom line. What matters is how quickly failures cascade, how effectively organizations anticipate interconnected impacts, and how resilient their operating models are when multiple risks materialize at once.

Three Focus Areas to Achieve Integrated Resilience in 2026

Only 20% of executives believe their firm is fully prepared to prevent or respond to outages, and 79% of organizations feel ill-equipped to comply with emerging operational resilience regulations, for which the EU has the strictest standards – NIS2, DORA, CER Directive.[7]

Drawing on commonalities across the rules and what we have seen among industry participants, here are three areas that will drive progress toward integrated resilience.

1. Mapping Critical Assets & Dependencies

Understand your infrastructure, how it is connected, and what is critical.

The most effective way to achieve this is through a single, centralized inventory that includes digital assets and the physical systems that underpin them.

A top-down approach to process mapping is the most efficient, starting with critical operations and working down to identify key dependencies. This creates a structured view of how essential services are underpinned, enabling more precise identification of single points of failure and concentration risk.

As best practice, organizations should document:

- End-to-end process maps, including key activities, decision points, and handoffs
- Human dependencies, such as roles, skills, and access requirements
- Technology enablement, including applications, data flows, integrations, and infrastructure components
- Physical infrastructure dependencies, such as facilities, power, cooling, and network connectivity
- Third- and fourth-party dependencies, clearly defining the services provided, contractual deliverables, and points of operational reliance.

7. https://www.cockroachlabs.com/blog/the-state-of-resgenuinelyilience-2025-reveals-the-true-cost-of-downtime/

INTEGRATING AI INTO ASSET AND DEPENDENCY MAPPING

Earlier in this paper, we highlighted the need for organizations to establish a centralized, dynamic model inventory to track AI model usage across the enterprise. Crucially, this inventory should be designed to inform the organization's broader infrastructure and process mapping from the outset, rather than being managed as a parallel or standalone exercise.

There is a clear opportunity to get this right from the start by embedding the model inventory into existing assets, processes, and dependency maps. Integration should be deliberate and foundational—not another silo layered on top of an already complex risk landscape. AI should be considered an extension of your existing risk management framework. This is what this looks like in practice.

This integrated view supports multiple regulatory and resilience objectives simultaneously.

Under DORA, it enables clear visibility into ICT dependencies and operational continuity. For NIS2, it strengthens network and systems resilience. Within third-party risk frameworks, it clarifies supplier dependencies, critical services, and SLA exposure. The EU AI Act adds further dimensions, including model type, use case, and risk classification.

2. Set and Maintain Impact Tolerances

Disruptions will occur, even in well-controlled environments. Impact tolerances define the point at which disruption becomes unacceptable, whether due to customer harm, financial loss, or systemic risk.

Practical approaches use time-based recovery metrics, such as recovery time objectives or service recovery objectives, alongside broader impact measures. These tolerances must apply not only internally, but also across third-party relationships, supported by enforceable SLAs, assurance activities, and joint testing.

Impact tolerances should reflect customer segmentation, potential loss severity, and reputational exposure, and be embedded into business continuity and incident response planning.

BEST PRACTICE:

- Define impact tolerances using multiple dimensions, including time, customer impact, financial thresholds, and reputational risk
- Align third-party obligations to recovery objectives through clear contractual terms and ongoing oversight
- Validate tolerances through realistic scenario testing. Bring third parties into joint test processes for which they are a key dependency

3. Invest in Training

74% of breaches involve a human element.[8]

As technical, physical, and AI-driven risks increasingly intersect, organizations require a more nuanced level of technical understanding to recognize how processes, systems, and third parties interact and how these interactions can amplify risk.

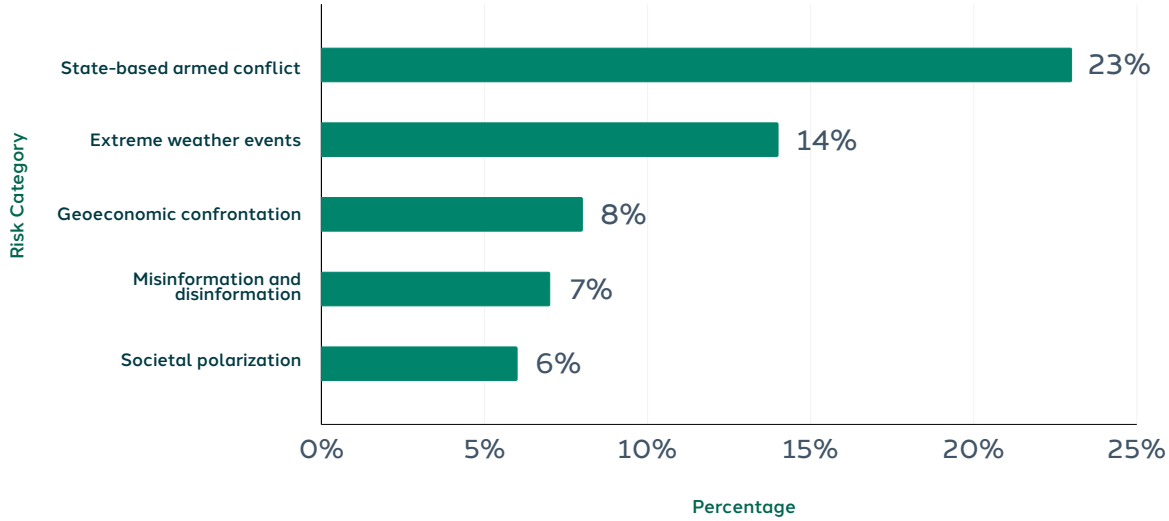
Upskilling senior leaders in this context enables clear prioritization, more effective investment decisions, and the cultural and structural changes needed to strengthen operational resilience. A strong, risk-aware tone from the top has never been more important.

People at all levels play a role in boosting a business's resilience. Firms should invest in targeted learning that supports both prevention and response. This means moving beyond generic annual training toward role-specific expectations, complemented by scenario-based and simulation-style exercises that help employees understand the real-world consequences of their actions during periods of disruption.[9]

8. https://www.verizon.com/business/resources/reports/dbir/
9. https://www.sai360.com/why-chief-compliance-officers-must-lead-the-culture-agenda

Geopolitical and Regulatory Uncertainty

Geopolitical and economic volatility have converged. Armed conflict, geoeconomic confrontation, and social polarization are persistent features of the global operating environment. The World Economic Forum Global Risk Perception Survey now ranks these as the top material global risks facing firms.



- *World Economic Forum - Risks most likely to present a material crisis on a global scale in 2025.*

At the same time, we have seen more regulatory fragmentation. While the narrative in Washington is shifting towards deregulation and reduced federal oversight, the lived reality for multinational firms is far more complex.

In the US, potential federal deregulation is being offset by state-level laws. AI provides a pertinent example – during the 2025 legislative session alone, at least 38 states adopted close to 100 AI-related measures.[10] Although recent executive action aims to consolidate AI governance into a single national framework, the pace and direction of change remain fluid.[11] The end goal may be greater simplicity, but the journey is volatile and resource-intensive to track.

This is all happening as Europe is pressing the accelerator. With DORA, NIS2, and the AI Act coming into force this year, even companies with no physical EU presence must be wary of EU standards for critical systems, third parties, climate disclosures, and AI usage if they sell into relevant jurisdictions.

The Strain on Compliance Strategies

Regulatory change and geopolitical risk are not new. What has changed is the environment in which regulatory and risk signals emerge. Several structural shifts are compounding the challenge for firms:

- **Expanded exposure through the extended organization:** Firms are more interconnected than ever. Deep reliance on third- and fourth-party service providers means more rules matter to more parts of the organization, even when they do not apply directly.
- **Deeper integration of technology into core operations:** Cloud infrastructure, AI, and global data flows underpin critical services across jurisdictions with divergent regulatory and political priorities.
- **Faster, noisier regulatory and geopolitical signaling:** the medium of delivery is changing. Policy intent, enforcement rhetoric, and geopolitical signaling increasingly surface first on platforms such as X, Truth Social, or regional social channels, often before formal guidance exists. These signals can move markets, trigger reputational risk, and pre-empt regulatory action.

In this environment, firms that rely solely on traditional sources like regulatory speeches, consultations, and published rules are already behind:

- 70% of organizations believe regulatory change will outpace their ability to adapt within three years.[12]
- “Keeping up with regulations” is the leading driver of rising GRC costs.[13]

10. https://www.softwareimprovementgroup.com/blog/us-ai-legislation-overview/#:~:text=On%20January%2023%2C%202025%2C%20President,in%20International%20Diplomacy%20and%20Security.
11. https://www.whitehouse.gov/presidential-actions/2025/12/eliminating-state-law-obstruction-of-national-artificial-intelligence-policy/
12. https://www.int-comp.org/insight/navigating-the-future-the-role-of-governance-risk-and-compliance-in-modern-business/
13. https://www.pwc.com/gx/en/issues/risk-regulation/global-compliance-survey.html#:~:text=It%20is%20not%20surprising%20that,consumer%20markets%20%2883

External Risk Intelligence is a Must-Have for 2026

Horizon scanning has grown in importance as regulatory and geopolitical complexity accelerates. Traditional approaches – periodic, manual, and narrowly focused on published regulations – have long been insufficient.

In 2025, many organizations adopted tools to automate horizon scanning and expand coverage. These solutions ingest a broader range of sources, including speeches, enforcement actions, and supervisory commentary, creating more dynamic, near–real-time feeds. In more advanced cases, regulatory obligations are extracted and accompanied by initial insight into why the change matters to the firm.

This is meaningful progress, but not enough.

In 2026 we will see an imperative to move toward more holistic external risk intelligence. Think of this as a unified, continuously updated view of regulatory, geopolitical, and economic signals that informs what firms need to do from a compliance and risk perspective.

In practice, this will be:

- **Broader:** Include sources beyond formal regulatory publications, such as non-legacy news channels and social media. And not just written content, but image and video, too.
- **Proactive:** More sophisticated sentiment analysis to identify early signals of intent before formal policy or regulatory action occurs.
- **Tailored:** Map external developments to the firm's specific business model, policies, controls, and third- and fourth-party exposures, and prioritize action accordingly.
- **Smarter:** Able to distinguish credible signals from noise, misinformation, and AI-generated content.

In 2026, external risk intelligence will be a baseline requirement for managing regulatory and risk signals at speed and scale.

Conclusion

2025 forced firms to confront the realities of operating in an environment defined by AI at scale, tightly coupled systems, and heightened regulatory and geopolitical uncertainty. Foundations were laid: clearer policies, greater awareness of interconnected risks, and early investments in automation and intelligence. The task now is to turn those foundations into something durable.

The emphasis in 2026 shifts from identifying risks to demonstrating that controls are embedded, repeatable, and scalable with the business. This will require an operating model that provides continuous visibility, faster insight, and more transparent accountability across people, processes, technology, and third parties.

For GRC leaders, 2026 is less about keeping pace with change and more about setting the conditions under which the business can move forward with confidence.

Emerging trends you need to stay ahead.

Find out more.

Our unified approach to risk sets us apart

Today's complex risk landscape demands more. SAI360 leads the way with an integrated GRC platform that spans the entire risk and compliance spectrum.

- Whistleblower and Case Management
- Ethics & Compliance Training
- Policy Management
- Conflicts of Interest
- Incident Management
- Regulatory Compliance
- Regulatory Obligations
- Horizon Scanning
- Enterprise & Operational Risk Management
- Third-Party Risk
- Internal Audit
- Internal Controls
- IT Risk
- Business Continuity
- Vendor Risk Management