IBM Platinum Partner

TECH mahindra

Balancing GenAI Innovation with Risk Management and Compliance

FEATURING RESEARCH FROM FORRESTER

Generative AI: What It Means For Governance, Risk, And Compliance

IN THIS DOCUMENT

Executive Summary

Today, enterprise leaders are part of a tight balancing act between delivering GenAI's transformative potential and navigating across constantly evolving governance challenges. The question everyone is asking is how to maintain the innovation velocity that competitive markets demand while establishing robust governance, risk management, and compliance frameworks that responsible deployment requires. While the stakes are considerable, there are scientific & methodological ways to deal with them effectively. This whitepaper examines how forward-thinking organizations resolve this paradox, presenting practical strategies that enable sustainable AI adoption without sacrificing regulatory compliance or stakeholder trust.

The GenAI Innovation Imperative

Every board meeting these days revolves around LLMs, agentic AI, and GenAI. What started as industry buzzwords just a few years back has now evolved into something resembling a technological gold rush. Every organization is scrambling to implement GenAI solutions, motivated by both genuine opportunity and competitive anxiety.

But truth be told, while everyone discusses revolutionary potential, it's only at the surface level. Only a few engage in the harder conversation about what production-scale success actually requires. In most cases, the primary barriers aren't technical or tool related. They're foundational, like trust, transparency, and governance, that prevent GenAI from scaling effectively. This reflects in our last two years' global customer engagement, and we call it the "POC (Proof of concept) trap"—that frustrating gap between impressive demonstrations and production systems that deliver measurable business value.

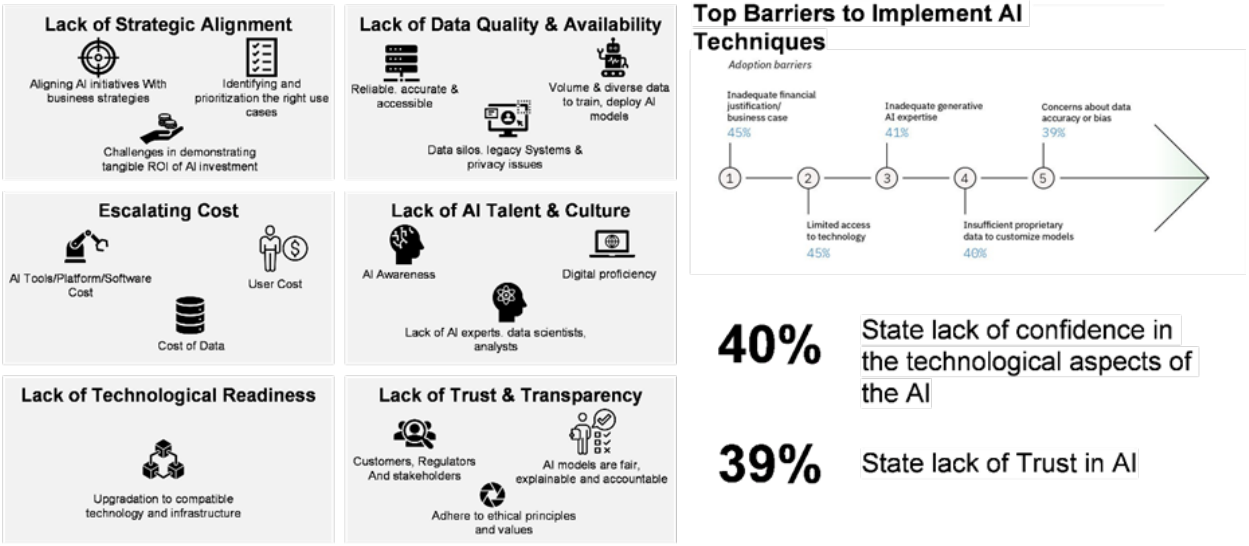
This implementation rush, while understandable, has created predictable failure patterns that transcend industries and organization sizes.

Why Most GenAI Initiatives Struggle

Our customer experience, combined with collaboration with IBM, has highlighted a key differentiator between AI leaders and laggards. The reality is that it is not about model sophistication or data lake size—but it is whether organizations establish comprehensive governance and validation frameworks from day one that enable proof-of-concepts to evolve into scalable initiatives.

Consider this reality: you can build an impressive GenAI prototype, but without the ability to explain decision-making, prove regulatory compliance, or guarantee production reliability, you'll remain stuck at the pilot stage.

This challenge extends beyond technical considerations—it's fundamentally about trust and responsibility. With agentic AI and advanced reasoning models, the requirement to explain AI decisions becomes even more critical.



When establishing governance for scale, we consistently observe two critical areas where organizations either succeed or fail:

1. **ROI Clarity:** Can you measure and demonstrate tangible business value from your GenAI implementation?
2. **Trust Establishment:** Do stakeholders—from end users to regulators—trust your AI systems enough to rely on them?

Trust in AI: The Real Governance Challenges Nobody Talks About

So, what are the common challenges of governance? Let's look at the comprehensive list below:

- **The Risk Management Reality:** Managing operational risks with AI systems differs fundamentally from traditional IT risk management. These systems can develop biases, drift from intended behavior, or fail in unpredictable ways.
- **Accelerating Regulatory Changes:** New AI compliance frameworks emerge faster than most organizations can track, particularly in Europe and the US. GRC professionals find themselves constantly reactive, struggling to stay current with global policies while building internal compliance capabilities. Missing regulatory requirements brings significant penalties and reputational damage.
- **Security Vulnerabilities That Keep Executives Awake:** AI systems introduce completely new categories of security risks: like unauthorized deployments, misconfigurations, prompt injection attacks, and data poisoning. The attack surface expands constantly. Traditional security frameworks weren't designed for these challenges.

- **Data Governance Complexity:** AI systems consume massive amounts of information for training and operations, creating challenges around data lineage, consent management, privacy protection, and cross-border governance. Mistakes here lead to regulatory sanctions and damage to the organization's reputation.
- **The Transparency Challenge:** Everyone discusses "explainable AI," but practical implementation proves incredibly complex. When AI makes decisions affecting customers, employees, or business outcomes, can you explain the reasoning? Can you confirm the absence of bias? Can you demonstrate accountability?

These challenges, while significant, aren't insurmountable. Leading organizations have developed practical approaches that address governance requirements while maintaining innovation momentum.

A Pragmatic Approach to AI Governance

GRC professionals' roles have transformed fundamentally in the AI era. They've evolved from cost centers focused on compliance checking to strategic enablers who help organizations capitalize on GenAI opportunities while managing risks intelligently.

Here's what our field experience shows works in practice:

- **Governance as Competitive Advantage:** Organizations that treat governance as a strategic enabler rather than a constraint achieve scaling success. They've learned to align risk management with business objectives, enabling progression from experimentation to optimization without compromising safety or compliance.
- **The Technology Platform Reality:** Manual processes don't scale; reactive approaches don't work either. Especially using spreadsheets and quarterly reviews for managing the AI governance risk should ideally move to a platform-based approach that delivers:

1. **Automated compliance and risk management:** Mapping regulations to internal policies, automating documentation, and reducing human error
2. **Real-time transparency:** Explainable AI processes, automated metadata capture, streamlined lifecycle governance
3. **Centralized risk management:** Unified repositories for regulations, risk data, and control assessments
4. **Continuous monitoring:** Real-time tracking of bias, drift, fairness, and unauthorized deployments
5. **Dynamic reporting:** Real-time compliance reports, model fact sheets, stakeholder dashboards

What We're Seeing in Practice

As practitioners working at the cutting edge of AI, we continuously test and evaluate emerging developments. Our observations:

- **The Implementation Gap:** Many organizations develop impressive GenAI prototypes but struggle with production deployment. The primary bottleneck isn't technical capability—it's governance readiness.
- **Regulatory Pressure Points:** Organizations in regulated industries feel increasing pressure to demonstrate AI governance capabilities. Those lacking robust frameworks find themselves unable to scale beyond pilot projects.
- **Security Reality Check:** AI security incidents become more common and visible. Organizations realize that traditional cybersecurity approaches prove insufficient for AI systems.
- **Cost Optimization Focus:** As initial GenAI excitement matures, organizations focus increasingly on cost-effective implementation and sustainable scaling approaches.

Practical Recommendations for Getting Started

Our field experience reveals what works:

- **Start with Governance, Not Technology:** Before implementing GenAI solutions, establish governance frameworks that can scale with your ambitions.
- **Invest in Platform Capabilities:** Manual governance processes don't scale. You need platforms that automate compliance, monitor risks, and provide real-time visibility.
- **Build Cross-Functional Teams:** Successful GenAI governance requires collaboration between IT, legal, compliance, and business stakeholders from the beginning.
- **Plan for Continuous Evolution:** AI technology and regulations evolve rapidly. Your governance framework needs adaptability, not rigidity.
- **Focus on Practical Value:** Governance shouldn't be a barrier to innovation. They should enable sustainable scaling of AI capabilities.
- **Learn from Others:** Partner with organizations that have production experience, not just theoretical knowledge.

THE IBM ADVANTAGE

IBM offers comprehensive tooling to help organizations address these challenges and overcome the complexities of AI governance and also named as a Leader in The Forrester Wave™: AI Governance Solutions, Q3 2025 with watsonx.governance.

IBM® watsonx.governance™ is an enterprise-ready AI governance toolkit designed to accelerate responsible AI workflows. It integrates seamlessly with existing systems, empowering businesses to adopt AI at scale. Moreover, it prepares you to meet regulatory requirements while optimizing costs. The key areas that watsonx.governance addresses are:

- **Compliance:** Simplify compliance by translating external AI regulations into enforceable policies that are automatically applied across systems. This helps ensure adherence during audits and compliance reviews while fostering transparency through factsheets that provide clear insights into model processes.

- **Risk and security management:** Preset thresholds in AI systems to monitor for bias, drift and breaches in key metrics and detect specific input/output content in real time. This proactively identifies and mitigates risks that could otherwise negatively impact the business. In integration with IBM Guardium® AI Security, you can preset identification alerts that flag unauthorized shadow AI deployments. It also unifies security policy across various teams—including risk, compliance and security—and provides visibility into vulnerabilities, misconfigurations and risk metrics.

- **Lifecycle governance:** Manage, monitor and govern any AI—model, applications or agents—whether developed using IBM or third-party platforms such as OpenAI, Amazon or others. Automating the model metadata capture simplifies report generation, while dynamic dashboards and visual reporting improve collaboration among stakeholders. Organizations can also streamline the evaluation of multiple AI assets simultaneously, accelerating time to production and automating AI governance.

IBM watsonx.governance provides the tools organizations need to scale AI responsibly and efficiently. Empower your business to unlock the full potential of AI with confidence. Simplify compliance, mitigate risks and streamline operations to build trust through transparency, save time with automation and enhance collaboration across teams.

THE TECH MAHINDRA ADVANTAGE

Tech Mahindra offers a distinctive advantage as a systems integrator with extensive experience building AI solutions from the ground up. The company prioritizes Responsible AI principles throughout its implementation process across the full spectrum of AI technologies, including Generative AI, Large Language Models (LLMs), Small Language Models (SLMs), and traditional AI development.

Tech Mahindra's VerifAI solution delivers comprehensive end-to-end verification and validation for AI projects. This enables customers to quickly adopt Responsible AI practices while leveraging established technology toolkits such as IBM's watsonx.governance.

Partnership Strategy for Effective Governance

GenAI governance complexity requires collaboration between technology providers and implementation specialists. Key aspects include:

- Technology Platform + Implementation Expertise: Robust governance demands more than technology platforms or expert consultants—success comes from combining advanced technology with hands-on implementation experience.

- Continuous Innovation: As AI landscapes evolve rapidly, governance approaches must keep pace. Strong partnerships build on continuous collaboration—enhancing capabilities and developing new solutions to address emerging needs.

- Industry-Specific Knowledge: Given diverse regulatory and operational landscapes across industries, successful governance requires tailored approaches—merging platform flexibility with deep domain expertise.

Strategic partnerships like the Tech Mahindra and IBM collaboration incorporate these essential aspects for effective AI governance deployment. These partnerships illustrate a critical principle: sustainable AI governance isn't built through vendor relationships alone, but through strategic alliances that evolve with organizational AI maturity and changing regulatory landscapes.

The Road Ahead

The GenAI landscape will continue evolving rapidly. New models will emerge with enhanced capabilities and reduced costs. Regulations will become more specific and stringent. Security threats will grow more sophisticated. Organizations that view governance as strategic enabler rather than compliance burden will be best positioned to capitalize on these developments. They'll adopt new technologies quickly, scale implementations efficiently, and maintain stakeholder trust throughout the process.

The era of sophisticated algorithms and ambitious claims has arrived. The future belongs to organizations that balance innovation velocity with governance rigor. This isn't about choosing between moving fast and being safe—it's about building capabilities that enable both. The question is no longer whether GenAI will transform business. But it's whether your organization will be ready to harness that transformation safely and effectively.

GenAI represents a fundamental shift in how we approach artificial intelligence, but success depends on our collective ability to implement it responsibly. Organizations that achieve this balance will define the next phase of AI adoption across industries.

TRENDS REPORT

Generative AI: What It Means For Governance, Risk, And Compliance

April 1, 2024

By Alla Valente, Cody Scott, and Heidi Shey with Amy DeMartine, Sudha Maheshwari, Kaylee Mahoney, and Peter Harrison

FORRESTER®

Summary

Global excitement, rapid adoption, and boundless possibilities for transforming all aspects of business thrust generative AI (genAI) into the technology limelight. But with a multitude of unknowns and little regulatory clarity, governance, risk, and compliance (GRC) professionals must step in to help their organizations navigate choosing the intended opportunities while avoiding the unintended consequences as they embrace genAI. This report is one in a series of Forrester research that aims to help business and technology leaders navigate the upsurge in generative AI.

The Impact Of Generative AI In Risk Management And Compliance

By its first birthday, ChatGPT turned genAI from a seemingly futuristic tool into the most widely adopted emerging technology since the debut of the iPhone in 2007. Today, tech giants like Google, Microsoft, and IBM vie for their large language models (LLMs) to be the foundation of every enterprise application, and smaller tech vendors race to embed genAI capabilities into their offerings to gain competitive advantage. GenAI's rapid evolution, coupled with the lack of clarity from US regulators and lack of standardization with global AI regulatory regimes, creates a multitude of unknowns. However, the potential benefits that genAI offers across the organization provide a rare opportunity for risk management to reinvent itself from the department of "no" to the discipline of "go." Led by the transformational chief risk officer, GRC pros are in a position to:

- **Identify which use cases have the biggest potential upside risk for the organization.** Forrester describes a fundamental shift in risk management from a transactional function that reduces costs to a transformational one that enables organizations to capitalize on new opportunities; make better, faster strategic decisions; and avoid unnecessary or costly missteps. This new focus puts risk management in the driver's seat to evaluate genAI use cases for undue risk, help apply genAI ethically, and identify what AI projects will require additional risk management guardrails, oversight, and controls. By focusing on outcomes, GRC pros can measure genAI's impact on customer experience risk, employee experience risk, quality, safety, and innovation, rather than simply the financial impact of a risk event or compliance violation.
- **Determine the optimal speed for genAI adoption.** Risk management and business alignment is key for helping organizations move from genAI experimentation to implementation — and then to optimization — faster and without endangering strategic goals or brand reputation. Alignment, along with trust and adaptivity, are the guiding principles of what Forrester defines as high-performance IT organizations, which achieve superior business results. Among these benefits is the ability to deliver new products for faster growth.
- **Shift compliance to the left.** In ideal conditions, compliance is the byproduct of effective risk management. But when it's treated as a standalone job, it inadvertently becomes a cost center. Organizations navigate a complex arena of standards, control frameworks, and regulatory requirements. With each of these requirements comes responsibility for developing reports, collecting metrics,

managing assessments, gathering audit evidence, and creating policies. GenAI shifts compliance to the left by automating manual compliance work, such as creating risk assessments, writing third-party questionnaires, monitoring real-time control status through integrations with enterprise technologies, and creating reporting tailored to the audience.

Early Benefits Of Implementing Generative AI For GRC

GRC pros are overwhelmed, oversubscribed, and constantly juggling risk and compliance requirements while also evaluating genAI risk and opportunities for the business. With the introduction of genAI, there's potential to ease the GRC burden by:

- **Identifying risks earlier.** Within the GRC process, risk identification is a laborious, multistep process. Some organizations take a top-down approach by starting with a framework or strategic objectives to identify potential risks. Others take a bottom-up approach by identifying risks based on audit findings, assessments, or alerts. Unfortunately, neither approach alone is sufficient, and the result is mostly reactive rather than proactive. Instead, genAI tips the scales in favor of proactive risk identification and uncovers unknowns where humans alone may not notice trends or cascading impacts. By leveraging integrations with internal business applications and external risk intelligence feeds, genAI will enable you to ask a digital assistant what your top potential risks are and provide contextualized scenarios to consider. For example, IBM OpenPages with watsonx allows users to specify a business area or objective and provides emerging risks associated with them based on its contextual analytics. Similarly, AuditBoard's new genAI capability helps users automatically draft risk statements and controls to move from identification to assessment.

- **Mitigating risks sooner.** When a controls assessment identifies that a control is weak or lacks the necessary maturity to adequately fend off potential risk, a mitigating control is introduced to reduce the chances of future failure, like a support beam to reinforce a structure and reduce the risk of collapse. Additionally, when a control fails outright, a compensating control is put in place to prevent risk. But how do we know which controls to implement and how successful they'll be at reducing risk? GenAI will recommend mitigating and compensating controls that meet specific regulatory requirements and leverage best practices based on the technologies and processes within an organization. For example, Workiva uses genAI to create remediation plan templates and stakeholder engagement plans, and Resolver uses its AI Intelligent Triage feature to help organizations mitigate emerging risks based on incident reports.

- **Modeling risk scenarios contextually.** Risk scenario analysis, the technique used for modeling and planning for unexpected events or changing risk conditions, has long been limited to historical data (i.e., what has gone wrong) and imagination (i.e., what could go wrong). GenAI removes those limitations and becomes a game changer for creating multifactored risk scenarios that account for emerging trends, new technologies, and geopolitical and economic fluctuations. Using contextual information about the organization, such as business model; geographic distribution of assets, customers, and/or partners; or changes in regulatory requirements; it can generate highly personalized risk scenarios or identify latent risks from low-probability but high-impact events, such as pandemics or unexpected product recalls. GRC pros can also use genAI to query data and discover the most likely emerging risks based on a variety of factors such as current events, geopolitical issues, and climate risk patterns.

- **Accessing policies, guidance, and training on demand.** One of the most common use cases for genAI is to enhance learning and make all employees be better risk managers. GenAI's ability to distill large volumes of information into straightforward summaries and find specific data points to answer a simple question means it is a perfect tool to reference policies, interpret guidance, and make risk-informed decisions quickly. For example, Johnson & Johnson and Cisco have expressed interest in using genAI to train and upskill employees on genAI. Among GRC vendors, SAI360 and NAVEX have introduced AI-powered assistants that answer employee compliance questions with information directly from policies and resources. These have the potential to transform the traditional employee help desk as well as expand assurance within the organization that policies and processes are upheld.

Act Now: Take The First Steps In Your Generative AI Journey

A Reuters poll found that 28% of employees regularly use ChatGPT at work, while only 22% say that their employers explicitly allow it. In Forrester's Data And Analytics Survey, 2022, 73% of technology decision-makers said that their firms were adopting AI, ML, or deep learning. And in Forrester's Priorities Survey, 2023, 62% of business and technology pros expected their firm to increase its AI investments in the coming year. The race is on to ensure that organizations have the means to guide the use of genAI for employees and within products and services. To adequately prepare, GRC pros must:

- **Revisit risk appetite to support, not bottleneck, their AI strategy.** Risk appetite is the level and types of risks that the organization is willing to accept in pursuit of its strategic goals and business objectives. Similarly, the risk appetite statement defines risk tolerance and expresses how much risk the organization is willing to take and at what cost, which in turn guides strategic decisions. When risk appetite is low, meaning the organization is risk averse, be prepared for adoption of genAI to be slower, but not impossible. GRC pros will need to prepare a well-documented business case for genAI and a clearly defined risk mitigation strategy. Ultimately, you will also want to review whether your current risk appetite is aligned with, or a bottleneck to, the goals and priorities of the business.

- **Create an AI governance framework.** This will be your organization's set of rules — policies, processes, and practices — for how AI can and should be used and to enable accountability for its use to ensure that it's responsible, ethical, and adheres to existing laws and compliance requirements. Globally, there are a multitude of frameworks for AI governance and risks. This complexity likely contributes to why, in Forrester's July 2023 Artificial Intelligence Pulse Survey, 34% of AI decision-makers at enterprise firms indicated that governance and risk are a major barrier to genAI adoption. Addressing privacy is a key component across many frameworks, such as the EU AI Act, NIST AI Risk Management Framework, and Singapore's Model AI Governance Framework. Getting AI governance right will require a balance of offense (deliver top-line impact) and defense (mitigate risk) in your approach.

- **Harmonize existing data use policies with genAI use cases.** GenAI interacts with data in three moments that define its risk surface: the prompt, the training of the model in use, and the output. Employees using genAI will likely want to use sensitive data, which could include personal data of customers and employees or corporate data like financial and proprietary information. Align data use policies to account for data use across these three moments as well as how genAI is deployed within your organization. Deployment can range from "bring your own AI" to training custom models. Employees need information about what data they can use with genAI and why. This also helps identify gaps where you must strengthen controls for data security and privacy to enable genAI use. As a part of this effort, you will also need to revisit your privacy policy and any contractual requirements or obligations associated with data use and handling. Ensure that policies do not contradict each other and that they are clear regarding genAI use and its interactions with data.

- **Establish guidelines for how third parties use genAI to support the organization.** In many organizations, genAI will come by way of third parties in the form of foundation models, pretrained data, open source LLMs, and new genAI capabilities of existing third parties. Humana, Cigna, and UnitedHealth all face class action lawsuits for their use of third-party software with AI algorithms that erroneously denied patient claims for services that physicians deemed medically necessary. All organizations are responsible and accountable for their use of genAI, even if it came from third-party tools. Ask the right questions when evaluating AI-enabled products; update the third-party assessment questionnaire to address privacy, security, and model risks; and ask for evidence. Validate that the way that third parties acquire, use, and train their AI models aligns with your risk appetite.

Don't Fall Victim To These Key Mistakes

As with any emerging technology, there are many unknowns that can lead to unforeseen or unintended consequences. However, GRC pros are already focused on mitigating the downsides, and many have tools and frameworks at their disposal to address the emerging risks of AI. GRC pros can't achieve genAI success if they:

- **Fail to keep abreast of global AI regulations.** The global regulatory landscape for AI is as diverse as the use cases it supports. With regions, countries, and jurisdictions all taking a different approach to regulating AI, GRC pros will need a comprehensive and coordinated approach for monitoring regulatory proposals, details of approved regulations, and milestones for compliance. Each regulatory regime will have a different goal for regulation, which translates to different requirements. For example, the EU AI Act aims to mitigate the potential harms of AI systems, rather than the technology itself. Japan's approach defers to the private sector's guidance and self-regulation of AI, while Canada's anticipated AI and Data Act focuses more on high-impact AI systems. Meanwhile, without US federal AI regulation, states and local jurisdictions pass their own regulations, which, to date, primarily focus on automated employment decisioning tools and algorithmic discrimination. GRC pros must understand the nuances of approved regulations and stay abreast of the evolving AI regulatory landscape.

- **Forget that use cases can run afoul of existing privacy and security regulations.** GenAI uses existing data and generates new content for use. As a result, there are plenty of present-day concerns where regulators and enforcement bodies will pursue violations that stem from how you use genAI. Antitrust and fair competition, consumer protections from algorithmic bias, and breach of privacy regulations like

GDPR impact AI and apply to AI even if AI isn't explicitly mentioned. For example, despite a lack of US federal regulations on AI, the FTC banned Rite Aid from using AI-based facial recognition for five years after the drugstore giant's previous AI-based surveillance led employees to falsely accuse customers of shoplifting. Similarly, Amazon landed a $25 million fine for violating child privacy when its AI voice assistant, Alexa, captured and stored voice recordings and location data of minors.

- **Neglect to update employees' acceptable use policies to include genAI.** At a minimum, revise general technology acceptable use policies to include genAI use, much like how you would address information handling and use of key tools like email, social media, and Wi-Fi. Firms encouraging its use should provide more detailed guidance and acceptable parameters in a standalone genAI acceptable use policy. As you develop such a policy, revisit existing policies — such as privacy, information security, and records retention — to assess them for alignment. It is also an opportunity to consider articulating your ethical principles as an organization to set an ethical AI charter. Follow updates to existing policy revisions or the rollout of a new genAI acceptable use policy with a refresh to employee training materials.
- **Don't align contractual language with their AI strategy.** Contracts are legally binding and enforceable agreements between you and your counterparties, which means that how closely your contracts, SLAs, and terms of use/service reflect your genAI strategy and updated policies will directly impact risk to your organization. An update to Zoom's terms of service sparked controversy when the new language gave the videoconferencing platform permission to use customer data to train its algorithms. Customer backlash led Zoom to reverse course, but it's far from the only tech vendor rushing to give itself permission to use your data to train its AI models legally. Work with contract management colleagues to review data use language in existing contracts and update contract templates to be compliant with the organization's AI policies. Use your contract lifecycle management solutions to flag changes to terms or other legal language that references key terms such as AI, models, algorithms, and data use.
- **Overlook recalibration of risk-reward tradeoffs.** By considering a broader range of scenarios and using generative models to assess their potential outcomes, risk managers can make more informed decisions to optimize risk-reward trade-offs. AI can affect a company in various ways, from internal operations to the products or services it sells. It is crucial for GRC pros to take a high-level perspective to identify all the ways that AI risk can impact their organizations by mapping it to prioritized use cases. GenAI can add tremendous value if the risk-reward trade-off calculations

are recalibrated to account for risk factors such as customer loss, reputational damage, and cost of litigation. For example, Air Canada is facing backlash and litigation after an AI chatbot gave a passenger incorrect information about its bereavement fare policy. Arguing that it wasn't liable for information provided by its chatbot didn't hold up in court and damaged the airline's reputation.

FORRESTER®

We help business and technology leaders use customer obsession to accelerate growth.

FORRESTER.COM

Obsessed With Customer Obsession

At Forrester, customer obsession is at the core of everything we do. We're on your side and by your side to help you become more customer obsessed.

Research

Accelerate your impact on the market with a proven path to growth.

- Customer and market dynamics
- Curated tools and frameworks
- Objective advice
- Hands-on guidance

Learn more.

Consulting

Implement modern strategies that align and empower teams.

- In-depth strategic projects
- Webinars, speeches, and workshops
- Custom content

Learn more.

Events

Develop fresh perspectives, draw inspiration from leaders, and network with peers.

- Thought leadership, frameworks, and models
- One-on-ones with peers and analysts
- In-person and virtual experiences

Learn more.

Contact Us

Contact Forrester at www.forrester.com/contactus. For information on hard-copy or electronic reprints, please contact your Account Team or reprints@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
Tel: +1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

Platinum Partner

ABOUT TECH MAHINDRA AND IBM

Tech Mahindra

Tech Mahindra is a global consulting service and systems integrator that operates in over 90+ countries, delivering solutions with a unique blend of digital innovation and robust, industry-strong processes. With our promise to help our customers Scale at Speed™, we design future state solutions for industry leaders and offer innovative digital experiences that enable them to transform and scale at speed. Our aim is to enable enterprises, associates, and society to Rise for a more equal world, future readiness, and value creation.

IBM

The mission of IBM is to be a catalyst that makes the world work better. We aim to have a positive impact globally, and in the communities where we operate, through business ethics, environmental commitment and responsible technology. For over a century, IBM has been at the forefront of technological innovation. Beginning in the earliest days of computing, IBM has blended intelligence, innovation and science to improve business, society and the human experience.

IBM is always on the hunt for what's next. Learn more about the group of more than 3,000 international scientists and researchers who believe in the power of the scientific method to invent at IBM Research, including leading the charge in quantum computing.

Contributors

Tech Mahindra

1. Nikhil Malhotra - Chief Innovation Officer | Global head of AI ((26) Nikhil Malhotra | LinkedIn)
2. Vinod Radhakrishnan - Head AI-Strategy and Growth ((26) Vinod Radhakrishnan | LinkedIn)

IBM

1. Soumitra Limaye - Director, WW Ecosystem Engineering | GSI Lab ((26) Soumitra Limaye | LinkedIn)
2. Balasubramani Radhakrishnan - Principal Business Technology Leader - Ecosystem Engineering Lab, Client Engineering ((26) Balasubramani Radhakrishnan | LinkedIn)