RISK MANAGEMENT

2025 RIMS Global ERM Award Winner 22

Criminally Overhyped: Risks of AI Washing 24

rmmagazine.com

2026 ERM special Edition



A publication of RIMS the risk management society

RIMS members **save up to $600** on registration

WHERE RISK GETS REAL

NEW ORLEANS2027
RISKWORLD®
APRIL 18-21
POWERED BY RIMS

Your people.
Your world.
Your conference.

The risk profession rewards those who stay ahead of what's happening, and that starts with knowing where the smartest minds in risk are gathering. RISKWORLD brings thousands of practitioners together to share information and strategies that keep judgement sharp.

Over four days in New Orleans, April 18-21, expertise is elevated for the current realities of risk: AI implementation, tariff exposure, alternate risk transfer, executive protection, global disruption. Relationships with peers and mentors are forged and chance encounters lead to new opportunities, including on the Marketplace Floor, where 300+ solution providers and welcoming spaces like the RIMS HQ Lounge make it easy to have productive conversations.

Learn more at
www.RIMS.org/RISKWORLD

contents

ERM Special Edition 2026 › www.rmmagazine.com



FEATURES

24 Criminally Overhyped: The Risks of AI Washing

It is not just overzealous marketing—businesses that make false and misleading claims about their AI capabilities can expose themselves to increased risk of litigation, regulatory scrutiny and other serious consequences.

30 How to Incorporate Tracking into Risk Management Processes

In addition to risk appetite, organizations must understand how much uncertainty they can accommodate, meaning an element is missing from the common 4Ts model: the deliberate decision to wait while closely monitoring a risk, or "Track."

WHAT'S INSIDE

4 Improving Organizational Sustainability Through Enterprise Resilience
Building enterprise resilience is not a theoretical exercise—it requires practical actions based on the current risk landscape.

8 Strengthening Risk Hygiene in the Face of New and Emerging Threats
As companies focus on new, headline-grabbing emerging risks, it is critical to ensure that they do not lose sight of foundational risk management practices.

10 The Human Barrier to Effective Risk Reporting
Building a culture where employees are comfortable raising issues makes the biggest impact in risk reporting.

12 How To Hone Your Risk Reflexes to Improve Risk Management
With these three practical strategies, risk leaders can build systems that enable business risk owners to learn and practice the right risk behaviors until they become second nature.



14 Key Risks to Address in AI Governance Programs
To best assess and mitigate risk, organizations must identify their exposure to these AI-related risks and account for them when developing guardrails for AI use.

18 Reputation Red Teaming: How to Design Immersive Crisis Response Exercises
Red team exercises ask companies to consider hot to establish narrative control in the first 48 hours of media coverage after a crisis.

22 Q&A: 2025 ERM Award of Distinction
Merline Barrington of the Port Authority of New York and New Jersey discusses the agency's award-winning ERM program and her journey as a risk professional.

COVER: GETTY/WESTEND61

RISK MANAGEMENT ERM Special Edition 2026 › www.rmmagazine.com

Editor in Chief
Morgan O'Rourke, *morourke@RIMS.org*

Managing Editor
Hilary Tuttle, *htuttle@RIMS.org*

Editor
Jennifer Post, *jpost@RIMS.org*

Art & Production Manager
Andrew Bass, Jr., *abass@RIMS.org*

ADVERTISING
Account Executive
Ted Donovan, *tdonovan@RIMS.org*
T: (212) 655-5917

A publication of RIMS the risk management society

Chief Executive Officer
Gary LaBranche,
glabranche@RIMS.org

AN AWARD-WINNING PUBLICATION

AZBEE AWARDS WINNER · EXCEL AWARDS WINNER · FOLIO: EDDIES WINNER · GD:USA AWARDS WINNER · TRENDY AWARDS WINNER

Zurich Resilience Solutions – Risk Advisory

Turning complex risk into informed decisions.



ZURICH
Resilience Solutions

As risks evolve and interconnect, risk managers and business leaders need clear, actionable insight.

Zurich Resilience Solutions combines **risk engineering** and **advisory expertise** to help you:

- Understand and quantify key exposures
- Strengthen operational resilience and supply chains
- Support strategic and board-level decision-making

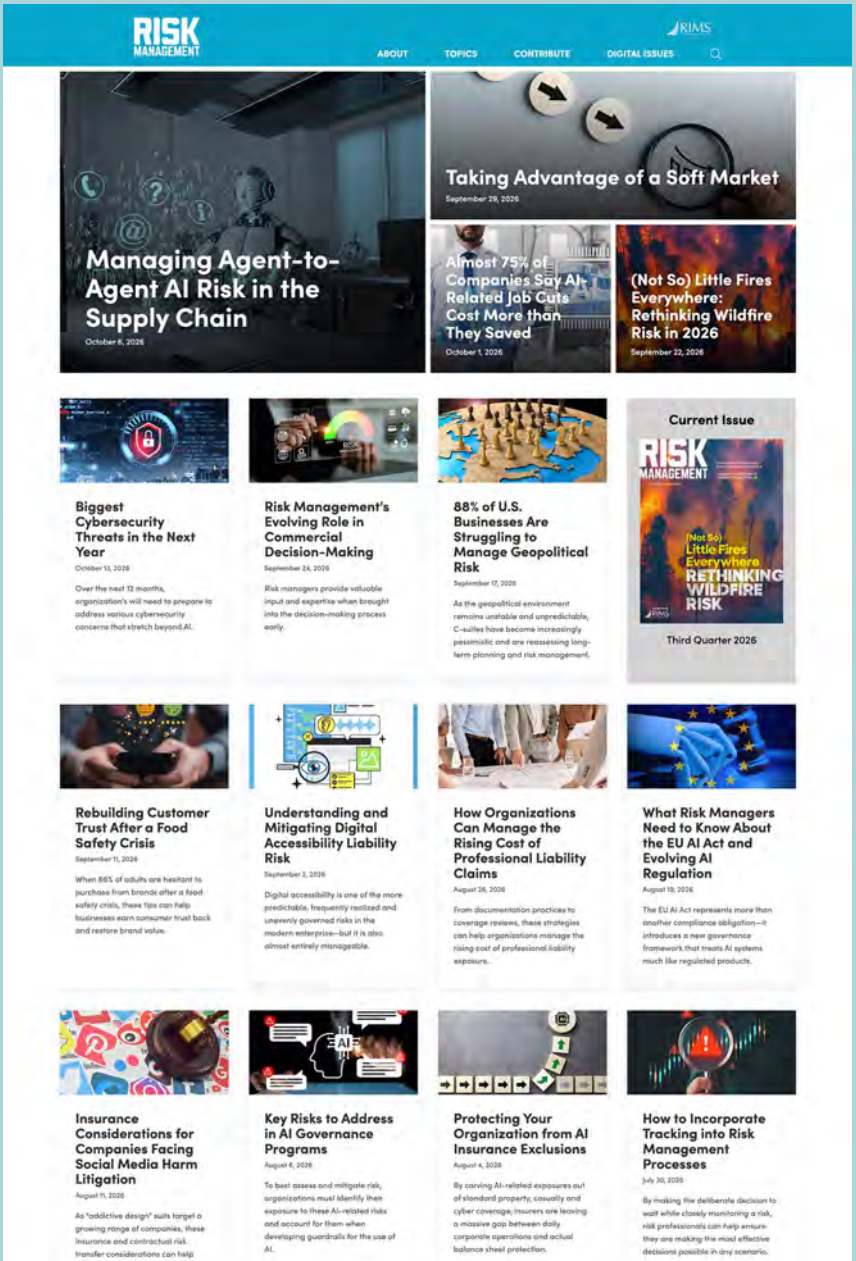
Whether you're focused on physical assets, critical operations or emerging risks, we work alongside your teams to translate complexity into practical strategies.

Meet tomorrow prepared.

Talk to the Zurich Resilience Solutions risk advisory specialists at the show
or visit: *us.zurichresilience.com*

Solutions and availability may vary by country and industry.

Whatever the topic, we have you covered



From fundamental resources to news you can use, *Risk Management* has a wealth of content to help risk managers stay at the top of their game. Check out the *Risk Management* website to browse resources such as:

- **Topics Index** to help you find articles on key subjects like Cybersecurity, ESG, Disaster Preparedness, ERM, Emerging Risks and Diversity, Equity & Inclusion
- **Online Exclusive Articles**
- **Current Issue,** including our Digital Edition
- **Archive of Past Articles and Back Issues**

Visit **www.RMmagazine.com** to learn more.

RISK MANAGEMENT



Improving Organizational Sustainability Through Enterprise Resilience

by Hazel Mak, Seet Yiwen and Teng Yi Sin

As organizations face continually expanding risks on multiple fronts, enterprise resilience has become a crucial foundation for long-term stability and ongoing success. At its core, enterprise resilience ensures operational continuity, sustainability and stability. However, true resilience extends beyond these basics, requiring organizations to be forward-thinking, responsive and creative in their approach. This iterative process is not merely about survival but also about continuously adapting, innovating and being agile in the face of disruptions to create opportunities for growth.

Enterprise resilience can be characterized by attributes in several core areas—digital, technological, operational, financial and talent—that collectively contribute to an organization's ability to withstand and effectively manage disruptions. Each is vital in building a comprehensive resilience framework.

- **Digital resilience:** An organization's ability to effectively withstand, respond to and recover from digital disruptions, such as cyberthreats or technological changes, defines digital resilience. It involves building the capacity, agility and skillsets necessary to manage severe cyber incidents. Key components of digital resilience include robust IT infrastructure, advanced cybersecurity measures, continuous adaptation to technological advancements, and the integration of flexible systems to maintain operational continuity and safeguard digital assets.
- **Technological resilience:** This refers to an organization's ability to create robust systems and infrastructures that capitalize on recent advancements. This can include investing in new tools, such as artificial intelligence and machine learning, to enhance operational capabilities and drive innovation. Technological resilience also involves maintaining a secure and adaptable infrastructure to prevent breakdowns and ensure continuity.
- **Operational resilience:** The focus of operational resilience is maintaining core business functions and services during disruptions. This attribute involves identifying critical processes, implementing contingency plans and ensuring resource availability to sustain operations. It emphasises proactive planning and preparation, including scenario testing, to effectively handle and navigate unforeseen challenges.

GETTY/BRENDAN SMIALOWSKI



- **Financial resilience:** This is the strength to withstand and recover from economic disruptions by effectively managing financial resources. It involves maintaining adequate liquidity, balancing short-term and long-term financial goals, and responding to shifts in the economic landscape. Key components of financial resilience include strategic financial planning and risk management, as well as the ability to adjust budgets and investments in response to market volatility.
- **Talent resilience:** Employees are the cornerstone of all enterprise functions, making talent resilience an integral aspect of enterprise resilience. This attribute refers to the capability of an organization's workforce to embrace change and work toward organizational success. It involves fostering a culture of learning, teamwork and creativity, as well as providing opportunities for professional development for a skilled workforce. Talent resilience is vital for building a motivated and agile workforce capable of navigating uncertainty.

Recommendations for Building Enterprise Resilience

Building enterprise resilience is not a theoretical exercise—it requires practical actions based on the current risk landscape. To enhance enterprise resilience, organizations should focus on several key strategies:

1. Integrate Resilience into the Risk Management Lifecycle

Modern organizations need to embed resilience as a foundational capability across all phases of risk management. This integrated approach establishes comprehensive frameworks for preparedness, responsiveness, adaptability and learning that directly support core resilience attributes.

Cross-functional risk reviews and scenario-planning exercises can allow organizations to examine interdependencies and stress-test assumptions, incorporating insights into workforce development programs and operational procedures. Regular simulations and drills should be woven into ongoing education to prepare teams for emerging threats.

Real-time data streams, predictive analytics and IoT-enabled dashboards can also help organizations continuously monitor treats and resilience metrics to support rapid, informed decision-making. This technology-enhanced approach enables early detection of emerging threats and facilitates coordinated responses across the organization.

2. Foster Adaptable Leadership and a Resilient Culture

Resilient enterprises begin with leaders who are agile, decisive and ready to navigate uncertainty. Adaptive leadership sets the tone for organizational culture, encouraging collaboration and openness to change. By promoting experimentation and viewing setbacks as opportunities for growth, leaders strengthen talent resilience by empowering teams and supporting a culture of innovation.

To support this, organizations should structure intentional leadership development initiatives focused on agility and scenario-based decision-making. Recognizing and rewarding adaptability and encouraging cross-functional collaboration can help dismantle silos and promote the sharing of critical information.

3. Invest in Continuous Learning and Targeted Upskilling

Continuous education and professional development enable staff to manage evolving risks, adopt new technologies and confidently respond to challenging situations. A workforce that values learning is better equipped to support digital, technological and operational resilience.

Conducting regular skills assessments that align with business needs, introducing user-friendly learning platforms, and promoting peer-to-peer knowledge sharing can drive this objective. By fostering a culture of continuous learning, organizations can equip their workforce for both anticipated and unexpected challenges.

4. Strengthen Communication Networks and Stakeholder Engagement

Proactive stakeholder engagement strengthens an organization's capacity to manage disruption by building trust,

clarifying roles and enabling coordinated action. Begin with stakeholder mapping to identify and prioritize key actors across internal and external networks, especially those whose decisions or actions are critical during disruption. Set clear expectations and maintain regular, purposeful dialogue that includes timely updates and structured feedback loops, ensuring that insights from stakeholders feed directly into decision-making processes.

Establish a robust communication network that connects all organizational levels and enables the rapid sharing of information, especially during times of disruption. Implement multichannel protocols for both routine updates and emergencies, with defined escalation paths to ensure critical information reaches the right people at the right time. Leverage digital communication platforms to increase transparency and real-time visibility and tailor messages to stakeholders. Develop pre-drafted, scenario-based messaging templates with placeholders, along with an expedited approval workflow and trained spokespersons, to enhance clarity and consistency during major incidents.

5. Establish Clear Measurement and Feedback Mechanisms
Organizations should establish meaningful metrics across all resilience attributes, such as recovery time and level for operational and technological resilience; system uptime for digital resilience; cash buffer days and current ratios for financial resilience; and role?specific pulse surveys on resilience areas such as stress management and collaboration for talent resilience.

Incorporating these measures into regular stress tests, simulations and post-incident reviews helps track progress, validate assumptions and uncover potential blind spots. Structured feedback gathered from these activities should inform policy, training and procedures for continuous improvement.

6. Tailor Resilience Approaches to Organizational Context and Maturity
Enterprise resilience works best when strategies reflect each organization's context, risk profile and maturity. Organizations should select and adapt tools to address operational risks, regulatory expectations and stakeholder needs, then test them in real workflows to validate relevance and effectiveness. Cross-functional input sharpens design and reveals blind spots, so bring these diverse perspectives early in the process.

Maturity matters as well. Run regular capability reviews against relevant standards or industry benchmarks to expose gaps and surface strengths that can be scaled. As markets shift, threats evolve and business models change, resilience strategies must evolve too. Plans, playbooks and metrics will need to be updated accordingly and anything that no longer serves its purpose retired.

7. Commit to Long-Term, Iterative Resilience Development
A sustained, iterative approach is essential for building enterprise resilience that endures. Organizations should secure ongoing support from senior leadership and embed resilience into strategic planning cycles, ensuring it remains a priority. Regularly review resilience strategies and adapt them in response to emerging risks, technological shifts and regulatory changes. Horizon scanning and periodic simulations can challenge assumptions and reward behaviors that identify potential threats and practical mitigations. Maintain a structured watch on regulatory and market shifts with routine benchmarking. Establish governance mechanisms to oversee resilience development, including defined ownership, review cadences and performance tracking. This disciplined cycle of review, learning and adaptation turns resilience from a one?off initiative into an enduring strategic advantage.

A Continuous Process

Embedding enterprise resilience requires integrating adaptable leadership, continuous learning, supportive technologies and a responsive organizational culture into every action. It is not a static goal, but rather a dynamic, multidimensional process that relies on organization-wide collaboration and customized strategies cultivated over time.

As risks and challenges continue to evolve, resilience should be embedded across all levels and strategies, with every employee understanding their role in anticipating, managing and learning from disruption. By embracing these principles—grounded in measurement, communication, stakeholder engagement and iterative development—organizations can transform resilience into a strategic advantage, allowing them to not only adapt and recover, but to ensure sustained success. R

Hazel Mak is the head of strategic risk management at the Office of Risk Management and Compliance at the National University of Singapore. **Seet Yiwen** is an assistant senior manager in the Office of Risk Management and Compliance at the National University of Singapore. **Teng Yi Sin** is an assistant senior manager in the Office of Risk Management and Compliance at the National University of Singapore.



Boost Your Risk Knowledge

Learn the ins and outs of trending topics at an interactive RIMS Virtual Workshop. Return to work with the confidence to apply your new skills.

RIMS-CRMP Exam Prep
January 27–28, 2027 | March 23–24, 2027
Prepare for the RIMS-Certified Risk Management Professional (RIMS-CRMP) exam with case studies and hands-on exercises.

Fundamentals of Insurance
February 10–11, 2027
Understand the basics of insurance, from insurance terms and concepts to what's included in a policy.

Risk Appetite Management
February 24–25, 2027
Learn how to develop a risk appetite framework that clarifies your company's position on risk taking.

Applying and Integrating ERM
March 3–4, 2027
Learn how to create and apply a practical ERM framework that builds and protects organizational value.

Risk Taxonomy for Effective Risk Management
March 11, 2027
Engage in hands-on exercises to align your risk taxonomy with industry best practices and organizational goals.

Creating Data-Driven Stories for Risk Management
March 17–18, 2027
Understand and apply the power of storytelling to effectively communicate risk management issues and recommendations.

Claims Management
April 6–7, 2027
Learn how to build a world-class claims administration program for your organization.

Managing Emerging Risks
April 29, 2027
Gain the skills needed to proactively identify, assess, and mitigate emerging risks.

View more upcoming workshops at

www.RIMS.org/VirtualWorkshops

RIMS
the risk management society

Strengthening Risk Hygiene in the Face of New and Emerging Threats



by Brittany Basler

According to the 2026 Allianz Risk Barometer, cybersecurity threats and artificial intelligence are the top global concerns for organizations across industries. These topics are at the forefront of today's headlines, and companies and executive-level leadership have understandably sharpened their focus on growth, control and risk management efforts in these areas.

However, when emerging risks consistently lead strategic conversations, a disconnect can develop within established programs and processes. Leadership must balance existing risk hygiene practices with the pressure of responding to emerging trends. Often, this effort is unsuccessful. The underlying issue is that while they are preparing for the future, they can unintentionally lose their grip on past controls and risk hygiene practices.

As focus shifts and risk hygiene erodes with time, it becomes a potential problem for companies and leaders. The erosion of risk hygiene is rarely dramatic or headline-worthy—until it is. It typically starts with subtle trade-offs happening in the background: A policy review is postponed, a training refresher is delayed or a compliance audit is pushed off. Eventually, years after a major emerging trend, exposure peaks because foundational hygienic practices have eroded as attention was directed elsewhere. Those small trade-offs sometimes snowball into undeniable exposure or liability.

Another gap occurs when focus shifts to an all-hands-on-deck approach toward emerging threats. As new risks demand the attention of executive-level leadership, resources and labor are often redirected to align with those goals. However, companies frequently fail to supply additional support to maintain existing operations. "Do more with less" becomes the unspoken mandate behind the scenes. Companies continue the balancing act with operational standards while simultaneously scaling into trending priorities.

New emerging risks should not force companies to abandon existing priorities due to restricted resources or inadequate risk hygiene processes. Organizations must preserve or clearly define foundations first, because emerging risks do not eliminate historical risks; they simply increase the complexity of managing them simultaneously. Once opportunities or gaps in risk hygiene are recognized, or when overload occurs without proper resources, companies have an obligation to their teams and to the preservation of business continuity to refocus and rebuild foundational practices.

By reinforcing core risk practices, companies can mitigate exposure even as new threats emerge. These key elements of proper risk hygiene can help organizations reinforce risk management fundamentals:

1. Implement inventory controls. Map existing policies, reporting

SHUTTERSTOCK/NA_STUDIO

pathways, vendor requirements and escalation procedures against how they function in practice. Written standards often differ from daily execution or become dependent on institutional knowledge. Over time, the informal shortcuts slowly replace structured processes when documentation is not present. When this happens quietly, organizations assume controls are working because documentation exists, even if execution tells a different story.

Conducting controls inventory can bring clarity. It forces organizations to examine whether policies are operationally applied or if they are just using best practices. It identifies where responsibilities overlap or where they are missing entirely, freeing up those needed resources. By establishing operationally applied programs and policies, companies can remove blurred lines that form when focus is redirected to emerging threats.

2. Assign ownership. Assigning ownership to critical areas of operation and risk exposure ensures that key risks continue to receive oversight even when leadership's time and resources are occupied elsewhere. Every major exposure area should have a clearly defined owner responsible for monitoring, validating and escalating issues. When no one is explicitly responsible for insurance tracking, incident trend analysis, training compliance or policy updates, those areas slowly lose attention.

Assuming ownership is present or having shared accountability can be just as dangerous as having no ownership at all and may lead to unintentional neglect. The purpose of defining ownership is not to place blame, but rather to create structural expectations and oversight in specific areas.

3. Establish review cycles. Quarterly reviews of claims data, vendor compliance, policy updates and incident trends reinforce discipline. Recurring review cycles are another way to establish preventative and retroactive expectations and ensure that important areas stay important.

Review cycles can also help with transitions. As organizations modernize systems, implement new technologies or adjust compliance frameworks, structured reviews help prevent legacy exposures from being overlooked. They ensure that antiquated processes are identified and corrected instead of being layered beneath new systems.

Review cycles strengthen documentation, validate consistency and identify patterns that may otherwise remain hidden. Most importantly, they add another layer of defined process, rather than purely operating off assumptions.

Ultimately, with the right foundation in place, leadership does not need to choose between preparing for the future and maintaining the past. Having foundational risk hygiene practices in place can allow organizations to focus on new threats while ensuring that historical or known risks do not reemerge in the background due to liability or operational breakdowns. R

Brittany Basler, MBA, is risk and safety manager for the City of Kissimmee, Florida.

Helping Risk Professionals Succeed in a Digital World

Access current and past issues of *Risk Management* for award-winning content about ERM, cyberrisk, natural catastrophes, emerging risks, insurance and pandemics.

Experience the best of *Risk Management* on your mobile devices today. Available at **rmmagazine.com**.



The Human Barrier to Effective Risk Reporting

by Maria Alexander



Most organizations have some form of risk reporting framework in place, with dedicated tools, policies and processes that explain what should be reported, when and how. On paper, these frameworks often look comprehensive. Yet, in many cases, important risks are discovered late or go entirely unseen.

When that happens, a pattern emerges that is familiar for anyone who has worked in risk or compliance long enough: Near misses go unreported. Clerical errors get quietly corrected. Software failures are handled informally within teams, and incidents appear in the system only if they happen to get escalated.

The problem is rarely the absence of a reporting system—it is what people associate with using it.

Why Risks Go Unreported

For many employees, reporting a risk can be uncomfortable. Some worry about how the information will reflect on them personally, who will see it, how it could be used later or whether it will trigger difficult conversations. Risk reporting often feels personal, especially when the immediate follow-up question after an incident tends to be "who was responsible?" instead of "what can we learn from this?"

In organizations where incidents have previously resulted in finger-pointing and blame, hesitation to report becomes a shared, unspoken norm. Employees learn that it is safer to handle problems quietly within their team than to escalate issues, even when escalation would provide clearer guidance and help prevent the same issue from happening again. Written policies may promote full transparency, but past negative experience shapes behavior far more than any mandate ever will. Over time, employees are conditioned to stay quiet, avoid drawing attention to problems and manage things internally.

This dynamic also affects how risk and compliance functions are perceived across the organization. Instead of being viewed as teams that enable and support business growth, they can start to be seen as purely focused on enforcement and control. Once that perception takes hold, employees begin to think that the act of reporting itself is risky. The gap between business teams and risk management grows wider, and trust erodes in ways that are hard to measure but easy to feel.

The Cost of Selective Reporting

Selective reporting not only leads to fewer reported issues, but perhaps more importantly, a distorted risk profile across the entire organization. Risk registers may show a tidy collection of minor events that people feel safe disclosing, while more complex or emerging risks remain hidden. Patterns that could have been identified early go unnoticed. By the time they are finally discovered, they are significantly harder to address.

SHUTTERSTOCK/BIGJOM JOM



When only certain risks are reported, the organization loses its ability to see the full picture. This weakens the foundation of how the risk appetite statement is set and how the risk appetite framework guides decisions. If leadership is making strategic choices based on an incomplete view of the risk landscape, then both genuine threats and valuable opportunities can slip through the cracks. The risk profile looks clean on paper, but it does not reflect reality.

Trust Over Policy

Risk reporting is not just a compliance requirement. At its core, it is a social process built on trust and fairness. People are more willing to report issues when they believe the response will lead to a discussion, not blame. When they can see a clear path for how their report will be used and understand why it matters, resistance drops.

This does not mean removing accountability. It means drawing a clear line between accountability and finger-pointing. A lot of this comes down to the educational dimension of risk management, the personalities of risk managers themselves, and the broader organizational culture that either supports or undermines open communication.

The risk management team sets the tone here. If that tone is prescriptive and top-down, where employees are simply told what to do and are obligated to follow established frameworks, people will start to see the risk team as an obstacle. If the tone is collaborative, where the risk team is approachable and willing to explain the reasoning behind the process and its benefits, employees will see them as partners who help the business succeed.

Making the Risk Team Visible

One of the most underrated strategies for improving risk reporting culture is simple visibility. Risk management should not be a faceless function that only shows up when something goes wrong. Risk managers need to be present, not just through the work they produce, but physically. Employees should know where to find them, recognize their faces and understand what they do day to day.

To help with visibility, risk teams should attend business unit meetings, not to audit or inspect, but to get a feel for what projects are in progress, what challenges teams are facing and what is on the horizon. Personal connections matter too. Small talk in the hallway, participation in team-building events or even just joining a lunch table can all help humanize risk teams. These actions build trust and connection in ways that no policy document can.

Fixing the Reporting Tools

Risk reporting tools play a critical role in whether employees actually use the system. The interface should be straightforward, with clear field names and a simple structure. Reporting a risk should never feel like a guessing game.

One way to combat confusion is to build company-specific templates. Many modern risk reporting platforms support this and even offer technical guidance for setting it up. Field names should be directly tied to the key risk indicators the company tracks for reporting and forecasting. It is also helpful to include clear descriptions of different risk types so employees can easily distinguish between a near miss and business as usual. Adding drop-down menus and relationship logic, where selecting a top-level risk category automatically narrows the options for the next level, can make a real difference in both speed and accuracy.

Education Beyond the Leadership Table

Another strategy that consistently delivers results is education, and not just for leadership teams or dedicated risk officers. The employees who need this training the most are the people performing operational activities, including customer-facing staff and back-office teams. They handle risk every day and they need to understand why reporting matters for the health and growth of the organization.

Regular training brings enormous value, especially when it is practical and consistent. Employees need to understand not only what should be reported, but what happens after the report is submitted. Uncertainty about what comes next often generates more resistance than the process itself.

Maria Alexander is a risk analyst in the financial services sector.



How To Hone Your Risk Reflexes to Improve Risk Management

by Tegan Gebert, Chris Audet and Doug Eckstein

Risk management is getting more attention from the C-suite, with Gartner surveys finding that 52% more CEOs cited it as a top priority for 2026 compared to 2025. The increase makes sense as organizations today face faster-moving, more interconnected risks that are increasingly shaped by technology.

Compounded by economic, regulatory and geopolitical volatility, the current operating environment makes traditional risk management approaches—where the core responsibilities of risk management are largely delegated to a central risk team—look increasingly inadequate. This is often because the central risk team is frequently alerted only after a risk has matured into an incident, which can then lead to other problems. For example, a cyber incident rarely stays confined to IT, often cascading into supply chain disruption, regulatory exposure and even talent fallout.

Business risk owners have the power and proximity to improve risk identification and response. However, Gartner surveys suggest that 88% of business risk owners are highly motivated to manage risk, yet only 35% feel confident in meeting risk ownership expectations.

This risk confidence gap is a structural vulnerability for organizations. When risk owners hesitate, wait for permission or treat risk processes as separate from "real work," it undermines the organization's ability to proactively and effectively manage its most critical risks in a coordinated way.

To bridge this gap, risk leaders must coach risk owners to recognize and respond to their risk responsibilities as quickly, thoroughly and autonomously as the current environment requires. That means creating risk management systems that enable business risk owners to learn and practice the right risk behaviors until they occur with such speed and precision that they appear reflexive. The following three practical steps can help businesses condition those reflexes.

1. Make Risk Ownership Hard to Avoid

Organizations tend to focus on making risk processes easier, for example, emphasizing streamlined templates, more accessible guidance or better tooling. The problem is that ease of use does not automatically improve risk owners' quality of work or level of engagement.

The key to conditioning a risk reflex is to make risk ownership hard to avoid. Hard-to-avoid systems compel action by being: prominent (hard to miss), useful (hard to justify ignoring), and visible (hard to hide avoidance).

SHUTTERSTOCK/IURII MOTOV, ROBUART

Ask yourself: Could someone be unaware of this process—or justifiably bypass this process—without anyone noticing? If the answer is yes, then its use is optional, in practice.

To put that into a practical example, imagine if your contract management platform was also your third-party risk gate. A contractor would be chosen from a pre-approved list of vendors that align with risk tolerance, and renewals would require embedded due diligence before they can be processed. In that design, the risk step is no longer "extra." It is part of the process.

Similarly, imagine embedding risk workshops into the transformation project process so that project teams were prompted to consider the timeliest, potentially high impact and high likelihood risks at each milestone. Embedding workshops into the process would make them hard to avoid, highly visible and clearly relevant.

Do not ask the business to "come to risk." Put risk where the business already is.

2. Provoke the Intellect

Reflexes also require stimulus. In risk ownership, stimulus is the moment where the risk owner is prompted to pause, assess and act.

If risk management wants better engagement or action from risk owners, then they must prompt or provoke the business with better stimulus. For example, think of the risk assessment process. Vague, surface-level risk assessment questions like "what are your biggest risks?" typically lead to vague, surface-level responses.

Consider how risk assessment questions can be designed to encourage more thoughtful responses:

- Ask questions that force specificity like "Are our objectives achievable, and what would cause us to miss them?"
- Explore cultural and information signals by asking "How open is management to hearing bad news, and what gets in the way?"
- Move from "Are controls in place?" to "What would break our controls under pressure?"

The goal is to receive better answers by asking more thoughtful, intentional questions. This idea is not limited to questions asked—it can also apply to how information is given or how meetings are structured. For example, risk management might capture leaders' perception of risk ratings through live workshops and a provocative prompt could be disclosing the risk ratings agreed upon in other, prior meetings. Disclosing contrasting risk ratings from prior discussions would challenge others' thinking and help them to engage or explain their reasoning more thoroughly.

3. Recognize Good Behavior

Reflexes are reinforced through recognition, yet most organizations tend to spotlight failure. Indeed, Gartner research found that only 22% of risk owners reported receiving positive feedback from ERM.

If risk management only measures and rewards "zero defects," it risks teaching the organization to hide weak signals—exactly the opposite of what modern risk demands.

Recognition starts with identifying what "good" looks like: proactive monitoring, early escalation, transparent communication, creative mitigation and learning from near misses.

Give visibility to risk ownership by having risk owners present mitigation plans to one another, sharpening risk thinking and creating healthy peer pressure to show strong preparedness. Use a dashboard to show executive leadership where risk owners are excelling with desired behaviors positioned to be emulated rather than ignored. Treat proactive risk behavior as a leadership competency and recognize it as visibly as performance outcomes.

Honing Your Risk Reflexes

In a world of interdependent risks and accelerating decision cycles, risk leadership cannot succeed through centralization and enforcement alone. The organizations that keep pace will be those that build reflexive risk ownership across the business with systems that are hard to avoid, interactions that provoke better thinking, and recognition that reinforces the right risk ownership behaviors.

By closing the risk confidence gap, you will not only improve your risk management processes—you can improve the speed, resilience and decision quality of the entire organization. R

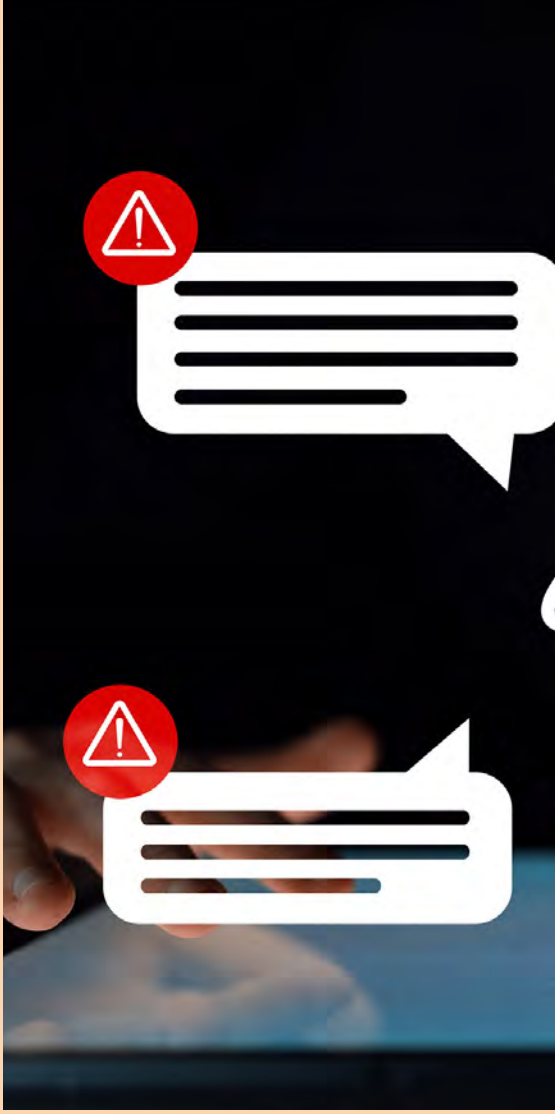
This article was based on the opening keynote at Gartner's 2025 Enterprise Risk, Audit & Compliance Conference.

Tegan Gebert is a vice president-level advisor in Gartner's assurance practice. **Chris Audet** is a vice president and chief of research within the assurance practice at Gartner. **Doug Eckstein** is a distinguished vice president of research at Gartner.



Key Risks to Address in AI Governance Programs

by Mark S. Goldstein and Regan M. Koski



Generative AI tools are now embedded in the daily workflows of many businesses. Employees use these tools to help draft emails, screen job applicants, generate marketing copy and analyze data. However, many business owners, executives and employees still have a limited understanding of the legal and privacy risks that can arise with every prompt. Developing a concise framework for identifying AI-related exposure can help organizations prevent violations before they occur.

Three overarching concepts should guide AI compliance programs: 1) human review is essential at every stage of AI-assisted work; 2) preventing AI-related violations requires affirmative action by employers, not passive hope that problems will not arise; and 3) the risks increase when AI-assisted creators profit, or seek to profit, from disputed work.

Businesses that fail to build compliance programs around these realities expose themselves to liability that grows with every unvetted output from an AI tool. Organizations that ignore the risks face serious consequences, including regulatory enforcement, civil litigation, reputation damage and the loss of valuable intellectual property. Companies that proactively establish compliance guardrails now will be far better positioned than those forced to respond to a crisis after the fact.

Key AI Risks Every Organization Must Address

To best assess and mitigate risk, organizations must identify their exposure to the following forms of AI-related risk and account for them when developing guardrails for the use of AI in the organization:

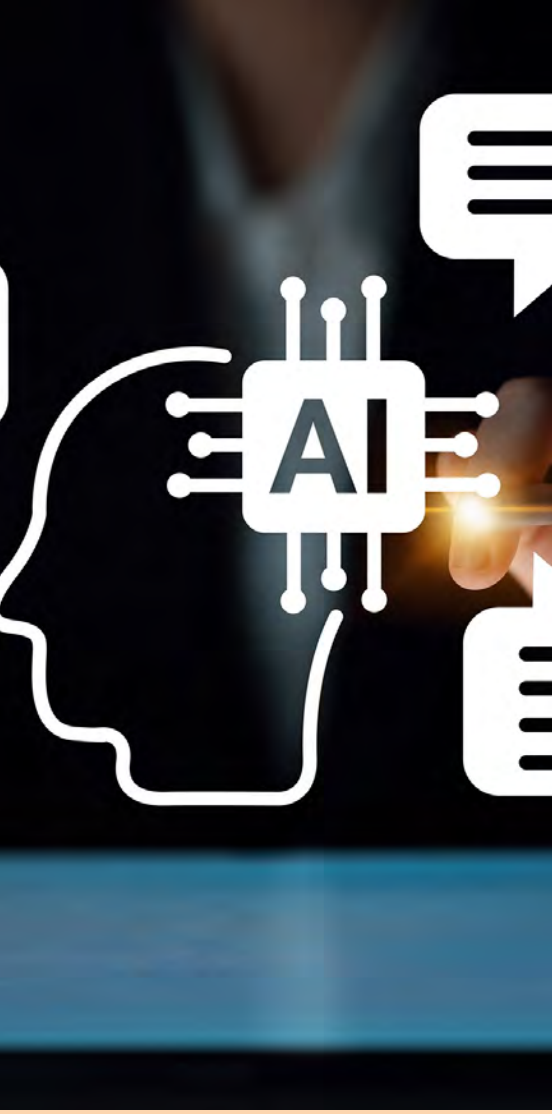
Confidentiality and Data Privacy

Workplace AI use can expose confidential client information or violate emerging AI and data privacy laws. There are many cases of employees uploading sensitive personnel data to public AI platforms. Others have incorporated competitors' proprietary materials into pitch decks and client presentations, unaware that the AI tool may have drawn from protected sources.

Employers must adopt clear policies defining permissible AI use, including training employees on which confidential information processing tasks must be restricted to internal AI systems and which may be handled on public, cloud-based platforms. Disclosures of salary data, personnel records, client information or other confidential business information may violate company policies and applicable law.

Employer AI training programs should ensure that employees understand their privacy obligations and the consequences of inadvertent violations. Before deploying any AI tool with sensitive data, organizations should thoroughly vet the tool's security protocols, data retention practices and compliance with applicable privacy regulations.

SHUTTERSTOCK/NA_STUDIO



Data Convergence and Visibility Controls

When personal and company data mix within an AI platform, employers are presented with critical questions: Who can see the information? What rules apply? How will the company prevent protected business information from leaking to unauthorized parties?

Employers should establish a triage system that identifies which tasks must be handled by internal AI systems and which ones can be processed on third-party platforms. Before deploying AI, the organization's legal, operations and IT teams should discuss where and how AI may be used, delineate approved platforms for different use cases and verify that policies work in practice.

Organizations should draw clear boundaries between personal employee AI use and corporate data handling. Ongoing dialogue among the legal, business and operations teams can help employees understand not only the rules but also the rationale behind them, which can help foster a culture of compliance rather than mere rule-following.

Internal Enforcement and Liability

Employees can be held liable or disciplined for how they use or misuse AI on the job. Employment policies should specify the consequences for failing to follow the firm's AI protocols. Organizations should also determine how liability will be allocated when a negligent employee creates legal exposure by ignoring AI policies designed to prevent trade secret, copyright or confidentiality violations.

Management should implement compliance checkpoints that preserve the benefits of AI while preventing uses that create liability. The cautionary tale of attorneys who submitted court filings with AI-hallucinated case citations for cases that did not exist demonstrates why multiple levels of human oversight are essential. One level of review is not enough.

Effective AI governance starts with a general policy statement on AI use, then builds a spectrum of acceptable uses and approved AI platforms based on project needs and data sensitivity. Employers should train all employees on what is permissible and maintain regular dialogue to ensure consistent implementation.

Intellectual Property Risks

AI is imperfect. It does not always identify source material, it is not always accurate and it can generate fictitious information. If AI-generated content ends up in products, brands or proprietary material, companies risk losing ownership rights. If AI-generated content includes the intellectual property of another and the company goes to market claiming the material as its own without proper vetting, the true owner may assert claims, particularly when the content is used for profit-seeking purposes.

Using AI-generated content for educational or internal purposes carries lower risk than incorporating the same content into commercial products or client deliverables. For internal use, the stakes may be manageable. The risk increases when confidential data, trade secrets or potentially infringing material is used in the marketplace to generate sales. Organizations should decide what safeguards are required before incorporating AI-generated material into valuable business assets, not after problems arise.

Important Employer Obligations

The same discipline applies beyond just intellectual property, particularly in employment decisions and other automated processes. AI's role in employment is expanding rapidly. Organizations use AI for sourcing candidates, screening job applicants, running background checks, conducting interviews, managing performance reviews, guiding employees to policies and benefits documents, and even selecting individuals for termination during workforce reductions. Generative AI is deployed across industries to translate documents, draft employment agreements and related documentation, and prepare workplace communications.

State-specific AI statutes increasingly target sectors such as healthcare, mental health services, insurance underwriting, civil rights and employment. Employers in these industries face heightened scrutiny and should be

particularly vigilant about compliance. For example, one bill being considered in Connecticut identifies the following best practices for employers to reduce the risk that bias and anomalies in AI systems will produce skewed employment outcomes:

- Inform an applicant or employee that the process is automated before they interact with a covered AI system.
- Provide written notice before collecting data and before making any AI-assisted decision. The pre-decision notice must explain what the system does, how the decision can be appealed and provide a link to the most recent bias audit.
- Ensure all final employment decisions undergo meaningful human review. An automated employment-related decision process may not be used in making a final or determinative employment decision unless a human reviewer has actual authority to change the outcome. Rubber-stamping the AI's recommendation is insufficient.
- Bring in independent, approved auditors to conduct pre-deployment and annual bias audits. Those audits must assess disparate impact against protected classes and test for less discriminatory alternatives.
- File and publish audit results with regulators. Critically, if the recent audit identified disparate impact, an automated employment process may not be deployed until the employer demonstrates legitimate business reasons and implements corrective actions.

> **"Businesses that fail to build compliance programs around these realities expose themselves to liability that grows with every unvetted output from an AI tool."**

The Path Forward

Guidance for businesses may become clearer as AI technology improves and legislatures define regulatory boundaries more precisely, but current restrictions are already here, and compliance cannot wait for perfect clarity. Human review remains essential to combat risks that AI cannot self-correct, including AI's failure to reveal its sources and its tendency to generate errors, fabrications and hallucinations.

The lack of a unified regulatory structure creates uncertainty for employers who must chart their own course without a clear model to follow. External enforcement will not be uniform as federal oversight remains in limbo. The field is instead governed by a patchwork of state-specific and industry-specific standards and laws. States like Colorado and California have enacted AI liability statutes, while others have no specific requirements.

For employers, the practical advice is straightforward: Follow the laws of the jurisdiction where the business operates and remain flexible. Build compliance programs that can adapt as the regulatory landscape evolves. Invest in human oversight as the non-negotiable foundation of AI governance. Above all, keep a human involved at every step to verify that AI outputs are accurate, properly sourced and do not infringe on the rights of others, especially when those outputs enter the marketplace in pursuit of profit. R

Mark S. Goldstein is a partner in Reed Smith's labor and employment group in New York. **Regan M. Koski** is an associate in Reed Smith's labor and employment group in San Francisco.

Stay Ahead of Tomorrow's Threats—Today

Risk moves fast— your insight should move faster.
Follow us for expert analysis, actionable takeaways,
and the intel leaders rely on to make smarter decisions.



RIMS-CRMP®

RIMS-Certified Risk Management Professional

Lead with Confidence

Earn the RIMS-CRMP Certification

In today's unpredictable world, organizations need risk leaders who anticipate, adapt, and deliver strategic value. The RIMS-Certified Risk Management Professional (RIMS-CRMP) certification proves you're that leader.

Whether you're advancing in your career or deepening your impact, the RIMS-CRMP:

- Validates your expertise in identifying and managing risk.
- Demonstrates your strategic value to leadership and stakeholders.
- Enhances your credibility with a globally recognized credential.
- Opens doors to greater responsibility and higher earning potential.

Trusted by risk professionals worldwide, the RIMS-CRMP is the only ANAB-accredited risk management certification in the world. Start your RIMS-CRMP journey today.

ANAB
ANSI National Accreditation Board
ACCREDITED
ISO/IEC 17024
PERSONNEL CERTIFICATION BODY

Learn More: **RIMS.org/Certification**

RIMS
the risk management society

Reputation Red Teaming: How to Design Immersive Crisis Response Exercises

by Ted Skinner



On January 5, 2024, Alaska Airlines Flight 1282 was flying at 16,000 feet when a door plug blew off the Boeing 737 MAX 9 fuselage. The two seats adjacent to the opening were, by chance, unoccupied. That stroke of luck is the only reason this incident did not become another mass casualty event for Boeing, a company still recovering from two fatal crashes that killed 346 people.

Within hours, the story dominated global news coverage. Boeing's stock dropped 18.9% in the following weeks, erasing more than $28 billion in market value. The FAA grounded all 737 MAX 9 aircraft with door plugs for three weeks, and Boeing's already tarnished reputation took another severe blow.

Six months later, CrowdStrike experienced a different kind of crisis when a routine software update crashed approximately 8.5 million devices worldwide that were running Microsoft Windows. Airlines grounded flights. Hospital systems stalled. Banks went offline. Emergency services encountered critical failures. The incident eventually cost insurers an estimated $1.5 billion in payouts and triggered legal action, including a $500 million lawsuit from Delta Airlines.

These two cases are instructive for risk professionals as they reveal an important disconnect in crisis management: Both companies had crisis plans, but neither was prepared for how the story actually unfolded.

Why Traditional Crisis Planning Falls Short

Most crisis management frameworks focus on operational response. Identify the problem. Contain the damage. Restore normal operations. Communicate status updates. These elements matter, but they miss something crucial: The headlines move faster than your operations.

In the first hours of any major incident, your organization does not control what the public sees. Journalists, social media users, employees and competitors are all narrating the story while you are still assembling your crisis team. The narrative gap between what is happening internally and what is being reported externally can determine whether a crisis becomes manageable or catastrophic.

Boeing's response to the door plug incident illustrates this problem. The company issued technically accurate statements, but those statements arrived after the public had already formed opinions. When CEO David Calhoun later told a U.S. Senate subcommittee he was proud of Boeing's safety record, the comment became its own reputation event, reinforcing existing negative perceptions rather than shifting them.

CrowdStrike faced a similar challenge. CEO George Kurtz's initial statement identified the problem and described who was impacted, but it did not include an apology. That omission became the story, overshadowing the company's rapid technical response.

SHUTTERSTOCK/GORGEV



As one communications executive observed, the first statement that travels widely shapes what people remember.

Implementing the Red Team Model

Military organizations have long used adversarial simulations to stress-test their strategies. The concept, commonly referred to as "red teaming," involves assigning a group to challenge plans by thinking like an opponent. The red team's job is to find weaknesses before actual adversaries do.

In the context of reputation risk, red teaming means testing crisis responses against realistic media scenarios before those scenarios become reality. The goal is not to predict exactly what will go wrong. The real objective is to build organizational muscle for managing the narrative dimension of any crisis.

Traditional tabletop exercises ask: Can we execute our operational response? Red team exercises ask a different question: What will the first 48 hours of media coverage look like, and are we prepared to compete for narrative control?

The Competitive Edge

Reputation risk management is not neutral. Your competitors are also managing their narratives, and a crisis for one company can become an opportunity for another. During the CrowdStrike outage, Microsoft's communications team worked to ensure customers and media understood that the problem originated with CrowdStrike, not Microsoft. That positioning was strategically sound, but it also meant CrowdStrike was fighting for narrative space against a much larger company with stronger media relationships.

Red team exercises should include this competitive element. How will your competitors describe your crisis? What will they say to your shared customers? How will you maintain relationships with stakeholders who are hearing alternative narratives?

Designing a Red Team Exercise

An effective reputation red team exercise requires different participants, scenarios and success metrics than a standard crisis drill. Consider the following steps:

1. Decide on participants. Start with the participant list. Traditional exercises often include operations, legal and communications staff. A red team exercise should consist of individuals who can authentically simulate external pressure, such as a skeptical journalist posing challenging questions, a social media commentator generating realistic commentary or a representative of a concerned analyst or investor.

These roles can be filled by internal staff from other departments or by external consultants, but they need enough distance from the crisis team to provide genuine pushback.

2. Detail realistic scenarios. Next, construct scenarios that prioritize narrative complexity over operational complexity. The most useful exercises involve situations where the facts are ambiguous, stakeholder interests conflict or the company bears partial but not sole responsibility for the outcome.

CrowdStrike's crisis is a good template. The company caused the problem, but the impact depended entirely on how customers had configured their systems. Who is the villain in that story? The answer depends on who tells it first.

3. Make timelines matter. Build your scenario timeline around media cycles. For example, the first impact might be a reporter calling for comment before you have confirmed basic facts. The secondary impact might be a viral social media post from an affected customer, and the third might be a competitor's statement expressing sympathy while subtly highlighting their own practices.

Each additional obstacle forces the team to decide: respond now with incomplete information, or wait and risk losing narrative control?

Running the Exercise

The mechanics of the red team exercise matter less than the pressure. Some organizations use detailed scripts with timed injections delivered through realistic channels. Others prefer a more fluid approach where facilitators adjust the scenario based on participant responses. Both can work as long as the exercise creates genuine decision points with real stakes.



During the exercise, make sure to document everything. Recording allows teams to review their decision-making process afterward, identifying where they hesitated, where they made assumptions that proved wrong and where internal disagreements slowed response time.

After the Exercise

After the scenario concludes, conduct a structured debrief that focuses on three key areas:

1. Review the statements produced during the exercise. Read statements aloud and consider how they would sound to someone without inside knowledge. Check whether they answered the questions stakeholders would actually ask or only the questions the company wanted to address.

2. Examine decision-making speed. Crisis communication often requires accepting 80% confidence rather than waiting for total certainty. Teams that struggle with this trade-off typically reveal the problem during exercises.

3. Assess coordination. Who had the authority to approve statements? Were the right people in the room? Did legal and communications work together productively, or did review processes create bottlenecks?

What Red Team Exercises Reveal

Organizations that run these exercises regularly report several common findings. Many discover that their holding statements are too generic to be useful. Phrases like "We take this matter seriously" or "We are investigating" do not satisfy anyone. Effective holding statements acknowledge specific stakeholder concerns and commit to specific follow-up actions.

Some find that their spokespeople lack practice in handling hostile questions. Reading a prepared statement is different from responding when a journalist asks why customers should trust you after an incident. That skill requires rehearsal. Others learn that their escalation procedures work well for operational decisions but poorly for communication decisions. A CEO may need to appear on camera within hours of a major incident. If the organization has not defined what triggers executive visibility, the decision-making process can become too slow.

Building Institutional Capability

One-time exercises can produce insights, but regular exercises build capability. Organizations that integrate red team scenarios into their annual calendar develop teams that respond to actual crises with practiced reflexes rather than improvised guesswork.

Consider scheduling exercises at different scales. Quarterly tabletop discussions may involve only the core crisis team and focus on specific skill areas, such as message development or media interview techniques. Annual full-scale exercises could involve senior leadership, external facilitators and scenarios that span multiple days of simulated time.

Rotate scenario types to cover different risk categories. Some should address operational failures, such as product defects or service outages. Others should explore external events such as regulatory investigations or activist campaigns. You could also add exercises that test responses to leadership crises, such as allegations of executive misconduct or sudden departures.

After each exercise, update your

SHUTTERSTOCK/GORGEV

crisis playbook based on what you learned. The playbook should include layered holding statements that can be adapted to different incident types, pre-approved messaging frameworks, clear escalation criteria and contact information for external resources that you may need to rely on under pressure, such as crisis communications firms.

How to Get Started

If your organization has not conducted a reputation red team exercise, begin with a focused scenario involving an incident that has actually affected a peer company. Use public reporting about that incident to construct a realistic timeline. Gather a small group of participants and work through the first 24 hours, producing actual draft statements rather than simply discussing what you would do.

This initial exercise will reveal gaps in your current preparedness. Use those findings to design a more comprehensive exercise with broader participation. Over time, build toward exercises that stress-test your organization's ability to manage not just what happened, but what people believe happened.

The companies that navigate crises most effectively share a common trait: They practice. Not just operational response, but narrative response. They thought about headlines before the headlines arrived. That preparation cannot guarantee a good outcome—some crises are genuinely uncontrollable. However, it can mean the difference between a crisis that damages your organization and one that defines it.

Ted Skinner is vice president of marketing at Fullintel and author of the book *Predictable Results: How Successful Companies Tackle Growth Challenges and Win.*

Verisk Maplecroft

Confident decisions start with better risk intelligence

Transparent external risk data and expert insight. Identify what matters, anticipate what's next and act with confidence.



With Verisk Maplecroft you can

Operationalize insights
Use common data across functions to assess exposure and coordinate decisions

Translate rather than transmit
Explain what has changed, where the business is exposed, how material the impact could be, and what decision is needed

Elevate external risk
Bring external risks to senior leadership when they could threaten strategic objectives or exceed risk appetite

Connect the risk landscape
Examine interactions across external risks to understand their collective consequences

Contact us info@maplecroft.com

Learn more maplecroft.com

2025 RIMS GLOBAL ERM AWARD OF DISTINCTION

Q&A: Merline Barrington ERM Program Director, Port Authority of New York and New Jersey



by Russ Banham

FOUNDED IN 1921, THE PORT AUTHORITY OF NEW YORK AND NEW JERSEY manages a complex regional infrastructure network with approximately 8,000 employees. The Port Authority oversees the world's largest airport system, the East Coast's busiest container port, the PATH rail system and the World Trade Center site. Operating in a high-stakes environment, the agency manages a diverse risk profile including capital project execution, climate resilience and cybersecurity threats.

The Port Authority's ERM program has evolved into a trusted agency function that informs strategic direction as well as operational and business decision-making through a risk-based prioritization process. By embedding risk-informed thinking into everyday business practices, the program has successfully fostered an enterprise-wide risk culture that breaks down operational silos across its diverse facilities and delivers measurable results that treat resilience as a core competitive advantage. In recognition of its success, the program received the RIMS Global ERM Award of Distinction in 2025.

Leading this ERM program is Merline Barrington, RIMS-CRMP, who sat down with RIMS to discuss ERM at the Port Authority, her risk management approach, and her unique journey to a career in risk.

RIMS: How did your early life guide you toward your career in ERM?
Barrington: I grew up in a diverse neighborhood in Canarsie, Brooklyn, in the early 1990s. Both my parents worked outside the home, so my grandmother was the primary caregiver. She spoke French, Creole and Spanish, but not English. I would translate for her at local grocery stores and negotiate prices on her behalf to reach her goal of paying the most affordable prices. These experiences taught me to assess a gap from various angles, identify the root cause of any misalignment and apply the most effective solution, even if that meant persuading my grandmother to select an alternative item or store. Leveraging my polyglot background in a close-knit immigrant family, I developed effective communication skills and a strong desire to help people overcome obstacles to reach their goals. This passion for advocacy eventually evolved into a professional focus on making things better at a structural level in public services on which people rely daily. I then obtained a master's [in Public Administration and Policy], aiming to impact large systems and government entities that affect our daily lives.

RIMS: What eventually brought you to the Port Authority?
Barrington: I learned through a mentor in graduate school about the Port Authority's Leadership Fellow Program, which is a highly selective two-year rotational program for graduate students interested in public service and management. Participants in the program work on various key projects for six to eight months in different departments, which appealed to me. I applied, entered the program in 2013 and transitioned into enterprise risk two years later, utilizing my public sector background. I have now spent a decade in risk, leading the division for eight years and culminating in my current role as the program's first director, reporting to the chief financial officer and the board of commissioners.

RIMS: What are some of the key factors contributing to the ERM program's success during that time?
Barrington: Since taking on the role, we focused on some key areas, namely, clarifying our value proposition to the enterprise, our formal link to strategy and strengthening risk analysis. To confirm and express our value proposition, we evaluated the agency's risk capabilities and the unique value of the ERM program by leveraging the RIMS Risk Maturity Model. This helps us understand risk management capabilities, how effectively risks are managed across the enterprise and identify areas for improvement over time. We also established a link to strategy by formalizing a top-down process that incorporates strategic priorities and goals, an executive-level risk committee with ownership of key risk areas, and an emerging risk practice. I also strongly believe in getting the job done and doing what you said you would. If I said I was going to help someone understand the cost impact of certain initiatives and inform resource allocation decisions, I am going to come back and tell you what I did and how I did it, which in turn strengthens the depth and relevance of risk analysis conducted.

RIMS: Are there any other key initiatives you would like to mention?
Barrington: One thing we did was establish executive-level ownership for risk areas through our dedicated executive risk committee, ensuring all chiefs are aligned with key risk areas. We then infused the ERM program with emerging risk research and analysis, proactively identifying uncertainties that can reveal opportunities. Now, we prioritize internal and external emerging risks to ensure strategic and operational resilience. We conduct research, collaborate on forward variables, and incorporate insights into workshops and meetings, challenging the status quo and expanding the risk dialogue, which I find exciting and vital for the agency's resilience.

RIMS: What are some of the ways you measure success?
Barrington: In addition to the RIMS Maturity Model, we conduct peer-to-peer benchmarking against comparable entities, which helps identify future focus areas, like leveraging AI for enhanced risk monitoring and insights. Feedback is big for me. We conduct several ERM workshops across the enterprise for frontline stakeholders, and I always reserve five minutes for participants to complete a post-workshop survey, easily accessible via a QR code we display during workshop closeout. This gives us feedback in real time.

RIMS: What challenges have you faced as you progressed in your role?
Barrington: Getting all the different departments on the same page about how we define and assess risks is an important contributor to our success. Every operation and business has their own culture and their own risk posture. We managed this by adopting a single way to talk about risk—a taxonomy. Then, we ran these cross-functional workshops to put the risks into context and prioritize them based on their financial and operational consequences.

RIMS: Aside from getting people to speak the same language about risks, how else do you foster a risk-focused culture?
Barrington: We exist within the context of business; any business issue is a potential opportunity to apply risk principles to close the gap. We build credibility and relevance by leveraging core business principles because risk manifests in the context of business. When engaging departments, for instance, we use tools like a business model canvas and KPIs. This gives us a firm grasp of their business and credibility. As the leader of this function, I am always on the lookout for their business needs and risks and how to close that gap.

Reporting is also critical, and I believe in reporting risk results to decision-makers on every level so that risk results are incorporated into decisions made on each operational and business level. The risk results that go to the board are strategic in nature—more significant overarching topics that call for the attention of board members and the decisions they can make. When we pick up on a potential issue and help leaders strategize how to fix it with risk principles, that is ERM winning and really propels the program.

RIMS: What excites you about the future of the ERM program?
Barrington: I am genuinely excited by the Port Authority's proposed capital plan and strategic direction because a lot of those major decisions were actually influenced by the agency's due diligence and consideration of risk. Now, I get to walk along with the enterprise to truly understand how that strategic direction unfolds and what risks might lie ahead. Guided by the COSO 2017 revised framework, we will continue to specifically link ERM with strategy and objective-setting. I am also excited to continue collaborating with executive leaders and being an even closer partner by demonstrating the organizational advantages of an ERM program.

Russ Banham is a Pulitzer-nominated business journalist and best-selling author.



Criminally Overhyped: The Risks of AI Washing

by Neil Hodge



In a climate where tech optimism is high, understanding is low, and regulatory oversight lags behind innovation, companies constantly seem to be making bold proclamations about how "next-generation artificial intelligence" has transformed their business and will push them ahead of competitors. Unfortunately, claims that seem too good to be true often are. Indeed, many businesses are either being misleading or even lying about the extent of their AI use, as well as the true capabilities and benefits of such technology.

For years now, many companies have been "AI washing"—a deceptive marketing tactic where companies exaggerate or fabricate their level of development or implementation of AI solutions to give the impression the technology is more pivotal than it is. According to Carrie Osman, CEO and founder of business consultancy Cruxy, AI washing is "a symptom of a market gripped by hype and starved of scrutiny" that is exacerbated by boards under pressure to "do something with AI."

"Every company wants to say they are using AI, but the hype has started to outpace the truth," said Ravi de Silva, founder of compliance advisory firm De Risk Partners. "We have seen this before with other tech cycles. There are big promises, fast funding and not enough oversight. The difference now is the speed of adoption and how deeply AI is being tied to valuations and business models."

Companies that engage in AI washing tactics can face serious consequences. By either deliberately or inadvertently misleading customers, investors and regulators, businesses expose themselves to increased risk of litigation and regulatory scrutiny and can needlessly increase their compliance costs as they provide assurance on risks that the technology does not actually pose.

Regulatory Scrutiny Ramps Up

In the United States, investor appetite to pour money into the "next big thing" has led the Securities and Exchange Commission (SEC) to step in to investigate false AI claims. In March 2024, the SEC issued its first enforcement action for AI washing, charging two investment firms with misleading clients and potential investors for years by pretending that their investment strategies were driven by a proprietary deep-learning AI model.

In June 2024, the regulator also charged Ilit Raz, the CEO of now-defunct AI recruitment firm Joonko with conning investors out of at least $21 million after enticing them with falsified testimonials about what the technology could supposedly do. According to a statement by Gurbir S. Grewal, director of the SEC's Division of Enforcement, Raz allegedly "engaged in an old-school fraud using new-school buzzwords like 'artificial intelligence' and 'automation.'"

In April 2025, the FBI and the U.S. Attorney for the Southern District of New York charged Albert Saniger, the former CEO of e-commerce firm Nate, with attempting to defraud investors out of $40 million by allegedly inflating claims about the supposed AI capabilities of its shopping app. In pitch materials transmitted to investors and venture capital firms, Saniger claimed the Nate app was "fully automated based on AI" and "able to transact online without human intervention." However, the app's actual level of automation was effectively zero. Instead, it relied heavily on bots and hundreds of workers manually processing transactions from a call center in the Philippines.

Even major technology companies have been exposed. In 2024, Amazon was lambasted after reports questioned the AI capabilities of the "Just Walk Out" technology installed at many of its Amazon

SHUTTERSTOCK/CKA

Fresh and Amazon Go grocery stores. The AI-powered system enables customers to pick their items and leave, with AI sensors allegedly working out what the shopper chose and then automatically billing them. Unfortunately, the cutting-edge tech also relied on around 1,000 workers in India to manually check almost three-quarters of the transactions. In response, Amazon said the reports were "erroneous" and that staff in India were reviewing the system, not the video footage from all the shops.

Meanwhile, Apple, Google, Microsoft and Samsung have been revising or retracting some of their claims about their latest AI products in response to a probe into whether marketers are overstating the capabilities or availability of AI features led by the national advertising division of BBB National Programs, a nonprofit industry self-regulatory organization.

The Federal Trade Commission (FTC) has also been monitoring how companies are using AI to mislead and lure consumers or investors into bogus schemes, and how the tech is being used to "turbocharge" fraud. In September 2024, it initiated a crackdown against misleading AI claims called "Operation AI Comply." The agency launched legal actions against various companies, including one that promoted an AI tool that enabled its customers to create fake reviews, another that claimed to sell "AI lawyer" services, and others that claimed that they could use AI to help consumers make money through online storefronts.

The agency made it clear that this kind of AI-driven fraud will not be tolerated. "Using AI tools to trick, mislead or defraud people is illegal," said FTC Chair Lina M. Khan. "The FTC's enforcement actions make clear that there is no AI exemption from the laws on the books."

Business Risks of AI Washing

While regulators have primarily focused on the risks to consumers and investors thus far, AI washing also poses several risks to the companies that engage in it. The most obvious risk is losing public trust in their products and brands by making claims that do not stand up. This can then result in a drop in sales and an increase in the threat of litigation and regulatory scrutiny.

Even unintentional misstatements can carry major consequences. "The legal risks are significant," said Maryam Meseha, partner and co-chair of privacy and data protection at law firm Pierson Ferdinand. "If a company's disclosures, whether in pitch decks, investor reports or public filings, materially misrepresent the role AI plays in their business, they may be liable for securities fraud, consumer deception or even FTC violations. We are already seeing the SEC scrutinize AI-related statements, and I expect enforcement to increase alongside new AI-specific disclosure rules."

It is important to note that companies are not the only ones that may face legal action—individuals within a company could also be sued, fined or face other regulatory sanctions for AI-related misstatements. "In investor agreements, there will often be warranties and possibly indemnities around disclosed information and breaching those terms could lead to damages claims—not just for the organization, but potentially for individuals too," Hall said.

Another risk is that companies could waste time, money and energy investing in solutions that do not deliver the benefits promised, making them wary about investing in future technologies and strategies that could actually pay off. "By chasing after hyped-up solutions, businesses may overlook genuine AI technologies that could truly drive efficiency and innovation within their operations," said Chris Carriero, chief technology officer at data tech firm Park Place Technologies. "The focus on superficial AI can blind organizations to the transformative potential of well-implemented AI and ultimately slow down their ability to adapt and thrive in a competitive landscape."

Another consequence of companies erroneously saying or believing they are AI-enabled is that they could be "unintentionally saddling themselves with a raft of compliance obligations under AI regulations," which will unnecessarily add to their costs for no apparent gain, said James Clark, data protection, AI and digital regulation partner at law firm Spencer West.

For example, the EU's AI Act, which was implemented in August 2026, states that "customers and regulators may legitimately assume that products referred to as 'AI' or 'AI enabled' constitute regulated AI systems." Under the legislation, companies deploying AI need to categorize how the technology is being used and assess the level of risk it could pose to the user. The higher the risk and potential for harm, the greater the company's compliance requirements will be. Adequately meeting these requirements can involve risk mapping to categorize AI applications according to the act's risk levels (unacceptable, high, limited, and minimal) and conducting impact assessments to evaluate how the AI processes data and whether the outcomes could lead to prohibited uses. To meet transparency obligations, companies will need to document decision-making processes, ensure human oversight where required, and implement audit trails. This could result in significant compliance costs, particularly up front.

Additionally, if a company uses the term "AI" when describing its products or services, "it may trigger a greater level of scrutiny from its corporate customers and third-party suppliers who will want additional assurances—and potentially stricter contractual terms and liability positions—to address perceived AI-specific risks," Clark said. As such, companies may be investing in sophisticated—and costly—AI compliance and governance

programs unnecessarily if their AI capabilities are minimal or non-existent.

Clearing Up Confusion and False Promises

At the heart of the problem is the lack of a universally accepted definition of AI and an inconsistent approach to regulation or enforcement. According to Ryan Gracey, technology and AI lawyer and partner at law firm Gordons, this "further fuels ambiguity and allows companies to stretch the term to cover a wide range of technologies, some of which do not meet the generally understood criteria for AI."

The most basic definition of AI is technology that can learn and evolve from massive amounts of data. But because some AI-associated technologies have been around for many years—semantic search and natural language processing go back at least a decade, for example—the term has become so broad that some businesses are even including technological processes as simple as automation under the banner of AI. Even in the European Union—which has led the way with regard to regulating the technology under the EU AI Act—the definition of what constitutes AI is open-ended. As a result, most corporate claims around AI "have enough of a basis in fact to evade regulation," said Tim Rosenberger, legal policy fellow at the Manhattan Institute.

Experts believe that the main reason companies tend to embellish their AI capabilities is that they see it as a harmless sales gimmick that is no worse than any other corporate boast. "AI washing is not often malicious—it is marketing teams getting ahead of technical reality," Meseha said. Joe Davies, CEO at content marketing and SEO agency fatjoe, said companies simply "leverage the term for clout, not capability" without thinking they are causing any real harm.

To prevent misleading claims, companies should play it safe and define AI technology as being at least capable of self-learning. "AI is generally understood to mean a method by which a computer can learn and solve problems further to training based on large datasets," said Iona Silverman, IP and media partner at law firm Freeths. "Anything less than that should not be labeled AI." Similarly, Melissa Hall, senior associate at law firm MFMac, said, "If the underlying tech does not genuinely involve AI, they should not say it does. It is that simple."

The key to avoiding accusations of AI washing is to



ensure transparency and accuracy when referencing the technology in marketing, investor materials and contracts. Companies need to ground their claims in demonstrable use cases. "Transparency is key," Davies said. "Disclose what AI is doing, where it fits in your workflow, and where human oversight still plays a role. Using terms like 'AI-assisted' rather than 'AI-powered' can strike a more honest balance."

Companies should make sure any AI claims can be backed up with solid evidence. "If companies are saying their AI product outperforms a non-AI product, they should have the data to prove it," Gracey said. "They must not make aspirational or hypothetical claims and should only talk about what technology can do right now."

Experts believe it is important for companies to have proper governance in place so that AI claims are not exaggerated and that everyone in the organization—from the board to sales teams—knows the difference between what can be deemed AI and what should be classed as generic, standard information technology. This includes training marketing and communications teams so that they understand what qualifies as AI and making sure all public statements are reviewed by the legal, compliance and other assurance functions. Companies should also maintain internal documentation showing how AI models were developed, validated and integrated.

According to business consultant Steve Fisher, companies need to build "internal literacy" to help combat the problem. "Executives, product leaders, and risk and compliance teams need a baseline understanding of AI—not to code it, but to question it," he said. "A company without AI fluency at the leadership level is vulnerable to both exaggeration and exploitation." Companies should create internal audit trails, ethics reviews and cross-functional reviews to evaluate both capability and risk. "If you would not let your security claims go unchecked, do not do it with AI either," he said.

Companies should also regularly review and update their claims as technology evolves, and if they are working with suppliers or partners, they should execute due diligence to verify those companies' AI claims so that everyone involved is clear about exactly what technology is used in the business and what the correct label for it is. Using established frameworks like the National Institute of Standards and Technology's (NIST) AI Risk Management Framework may provide a blueprint for companies to follow, but organizations should also ask themselves a series of questions to avoid using "AI" as a catch-all term for technical investment. These should include: Is what we are building truly autonomous? Are human decisions being disguised as algorithmic ones? Who might be harmed by our claims?

Despite the increased scrutiny, AI washing is likely to continue with more companies exposed to reputational risk and legal hazard from false and misleading claims. Zorina Alliata, principal AI strategist at Amazon and professor of responsible AI at the Open Institute of Technology, believes companies need to treat AI washing like they would any other product risk. "We can ask investors and stakeholders to expect technical due diligence, boards to take AI claims as significant disclosures, and C-suites to educate themselves and understand the opportunity—but also the limitations and hazards—the technology brings." R

Neil Hodge is a U.K.-based freelance journalist.

Here, There & Everywhere

Risk Management is always a click away with the information you need to stay ahead of the curve.

To check out the latest articles, browse our archive and read exclusive online content, visit us at **RMmagazine.com**.





Amplify Your Voice

Share your expertise and perspective with your peers and help create a stronger and more vibrant risk professional community by contributing to *Risk Management*.

Visit **RMmagazine.com/contribute** for details on how you can get involved.

RISK MANAGEMENT



SHUTTERSTOCK/MINISTOCKER

How to Incorporate Tracking into Risk Management Processes

by Dr. Jon McNeill and Dr. Dominic Duckett

Some of the most effective business decisions come from deliberate restraint rather than rapid action. For example, risk professionals often face pressure to take decisive action to "return to normal" even when conditions remain uncertain, while the most prudent response would be to actively monitor the situation until the picture becomes clearer.

The 4Ts model of Tolerate, Treat, Transfer and Terminate remains a central framework for risk response and appears in standards such as ISO 31000 and COSO ERM, but the 4Ts may not fully reflect what organizations do in practice. Organizations must understand not only their appetite for risk, but also how much uncertainty they can accommodate. In this context, an element is missing from the 4Ts: the deliberate decision to wait while closely monitoring a risk, or "Track." This distinct strategic response could be considered the fifth T. By incorporating Track into their risk management process, organizations can help ensure they are making the most effective decisions possible in any scenario.

Why "Track" Matters

At first glance, adding another category to the 4Ts may not seem necessary. Monitoring is already a key part of risk management. Risk professionals update registers, review controls and reassess risks, but this usually accompanies another response. They treat, transfer or tolerate a risk, then monitor to ensure the response remains appropriate.

However, tracking is different. It is a deliberate choice not to act yet because conditions are too uncertain, information is too limited or timing is not optimal. It is a temporary holding strategy that preserves flexibility while circumstances evolve.

Formalizing Track as part of risk response matters because many environments are fast-changing and information often emerges gradually. Premature action can close off better options or shift risk elsewhere. In such cases, waiting is not passive—it is disciplined and accountable, especially when knowledge is incomplete.

A practical starting point to incorporate Track into your risk response process is to review your current risk register and identify risks where immediate action is hard to justify. These are typically high-uncertainty risks with multiple possible outcomes or dependencies on external decisions. If you find yourself repeatedly deferring action without clear reasoning, it may be a sign that the risk needs structured tracking rather than indefinite postponement.

The Most Under-Used "T"

To understand why Track is underused, consider two linked challenges: 1) the action bias that pushes for early decisions and 2) the hindsight bias that punishes restraint once events unfold.

The Action Bias Problem. Recommending "wait and see" is difficult within organizations that prize visible action. Risk managers feel pressure to demonstrate they are doing something, and this can distort priorities, consume resources prematurely and create a false sense of progress.

Because activity is often valued more than judgment, professionals may hesitate to propose strategically waiting even when they believe it is the most prudent option. Many fear the stigma of being seen as indecisive or insufficiently proactive. However, decisions often involve a trade-off between moving forward and gathering enough information to act well. Track provides a legitimate label for this disciplined pause by reframing a delay as a conscious, time-sensitive response to uncertainty, grounded in professional judgment and supported by clear escalation conditions.

The Hindsight Problem. Every Track decision may eventually face hindsight bias. Fear of retrospective criticism encourages premature decisions that appear decisive even when suboptimal, while patient tracking is punished regardless of its merit at the time. The consequence is that once outcomes become clear, critics claim they "knew all along" what should have been done.

To best prepare for this tendency, practitioners should document reasoning at the point of decision, including what was known, what remained uncertain and what triggers would prompt action. It is equally important to make sure you do not engage in hindsight bias yourself. Judge past decisions based on the information available then, not by later events. A well-structured Track response that produces a suboptimal outcome may still be better risk management than a lucky guess or premature action.

What Track Looks Like in Practice

Track already happens informally and can be either active or passive. Understanding this distinction helps explain how it differs from the existing 4Ts.

Consider the analogy of a goalkeeper facing a penalty shot. Goalkeepers who choose not to move during penalty shots have higher success rates than those who dive, even though this appears counterintuitive to spectators who expect immediate action. A goalkeeper deciding in advance to stand still based on statistical analysis represents a classic Tolerate approach from the existing 4Ts.

Track is different. Rather than committing to a specific strategy in advance, the goalkeeper would delay their final decision, actively monitoring the penalty-taker's approach, body language, run-up angle and hip positioning. This preserves multiple response options until the moment when maximum information is available. The key distinction is timing and intent. Tolerate means accepting the risk itself because other treatments are not appropriate, whereas Track keeps all treatments open and deliberately postpones the choice while conditions continue to evolve.

The U.S. Federal Reserve's 2012 deliberations offer a masterclass in active Track. As the economy nursed wounds from the recession, Federal Reserve Chairman Ben Bernanke faced intense pressure. Hawks like Richmond Fed President Jeffrey Lacker warned of inflation risks from continued quantitative easing. External voices like economist Paul Krugman urged patience, while financial media warned the Fed was behind the curve. Rather than setting predetermined thresholds and waiting passively for them to be breached, like a stop-loss order in currency markets, the Fed employed active Track. They did not simply monitor inflation and employment against fixed targets; they continuously recalibrated their understanding of what "full employment" meant in a post-crisis economy, adjusted their assessment of inflation risks as global dynamics shifted, and evolved their communication strategy as markets digested each round of quantitative easing. When labor force participation rates fell unexpectedly, they reconsidered whether traditional metrics still captured economic slack. This active tracking, including constantly reassessing both the risk and the response thresholds themselves, allowed them to maintain appropriate policy longer than passive triggers would have permitted.

Track is particularly useful for interdependent risks. Modern risks often cut across departments, supply chains and jurisdictions, and acting too quickly in one area can

have unintended consequences elsewhere. Tracking enables coordination and time for wider consultation before decisions become locked in. Most complex risks benefit from a blend of passive metrics and active contextual monitoring.

A Four-Step Process for Implementing Track

For Track to function as a fifth T in practice, it must be structured. "We will keep an eye on it" is not enough of a strategy. A responsible tracking process includes four key steps:

1. **Recognize when Track is appropriate**
To recognize when Track is the appropriate response, look for situations where volatility dominates, information remains incomplete or premature action could lock the organization into suboptimal paths. In such cases, inaction today can preserve the freedom to act more effectively tomorrow. For example, during political transitions, manufacturers may choose to delay operational changes because committing to any regulatory framework while conditions are fluid risks costly error.
2. **Define what you are tracking and how**
Once you decide to track, define what you will monitor. Identify the variables that matter most, the sources of reliable data and the frequency of review. For example, a consumer goods firm facing supply chain uncertainty might track policy announcements, logistical cost changes and competitor adjustments. This should turn vague watching into systematic observation.
3. **Establish review timelines**
Next, look to establish clear timelines and triggers to prevent drift. Tracking must remain provisional. Effective triggers might include numerical thresholds, competitor actions or specific regulatory milestones. Examples could include a 15% price shift, two major competitors adopting a new standard, or a 10% increase in enforcement action.
4. **Communicate rationale and escalation conditions**
Finally, communicate the rationale. Stakeholders should understand why Track was chosen, what conditions would prompt a shift and how updates will be provided. An initial message might explain that Track preserves flexibility until key uncertainties resolve. Subsequent updates can confirm whether triggers have been met and when the next review will occur. If escalation is needed, communication should be clear and decisive.

How to Ensure Discipline in Tracking

For tracking to function as a disciplined strategy rather than a convenient holding pattern, these habits are essential:

Revisit tracked risks regularly. Rather than being left to drift, ensure risks receive scheduled review and adjust triggers and thresholds as new information emerges. Tracking must remain active and cannot slip into set-and-forget mode.

Communicate the rationale clearly. Those overseeing the risk should understand why Track was chosen, what variables are being monitored and which indicators would trigger a shift in response. Clear explanation should help stakeholders understand you are acting with deliberate caution, not indecision.

Avoid waiting for perfect information. No matter how much research you do, many risks are likely to include some element of uncertainty indefinitely. Track is not a justification for indefinite delay when uncertainty is not reducible.

Approach tracking with rigor rather than avoidance. Track should never become a way to park uncomfortable issues or postpone decisions because action is politically awkward. Tracked risks still require engagement, documentation and periodic reassessment.

Risk professionals are often expected to advise, intervene and act, but sometimes it is better not to act immediately. The value of tracking lies in the idea that timing is a core competency in risk management. Its relevance is greatest where uncertainty is expected to decrease, where conditions are still forming, and where premature action would close off better options.

Next time a risk surfaces and the urge to move quickly takes over, ask yourself:

- Is this a risk where key uncertainties are genuinely time sensitive and likely to resolve?
- Is our reluctance to wait grounded in uncertainty or fear of looking passive?
- Are we acting because it is the right decision or because it is visible?
- Would stepping back actually serve the organization more effectively?

Bringing Track into the 4Ts framework is not about slowing down—it is about thinking ahead. It applies where waiting is likely to improve the quality of information or reveal clearer pathways, giving risk professionals permission to pause, observe and preserve options. In a world where risks evolve quickly, Track can help organizations align decisions with clarity rather than urgency. R

Dr. Jon McNeill is program leader and lecturer for risk management in the Department of Finance, Accounting and Risk at Glasgow Caledonian University's Glasgow School for Business and Society. **Dr. Dominic Duckett** is a lecturer in risk management in the Department of Finance, Accounting and Risk at Glasgow Caledonian University's Glasgow School for Business and Society.