RISK MANAGEMENT

ERM Special Issue 2025 RMmagazine.com

Optimizing your Enterprise Risk Management Strategy pg. 2

How to Overcome Cognitive Biases in Risk Management pg. 20

2025 ERM Special Edition

A publication of RIMS the risk management society

Advance Your Risk Management Skills Virtually

Enhance what you learned at the RIMS ERM Conference by continuing your professional development through a RIMS Virtual Workshop. These expert-led sessions dive deeper into key risk management topics, helping you build on the insights and strategies you gained in Seattle—all from the convenience of your screen.

Workshops include:

- Applying and Integrating ERM
- **New!** Emerging Risks
- **New!** Intro to ERM for Senior Leaders
- Managing Data for ERM
- Optimizing Risk Management with Artificial Intelligence
- RIMS-CRO Certificate Program in Advanced ERM with James Lam
- Risk Appetite Management
- **New!** Risk Taxonomy for Effective Risk Management

Join a RIMS Virtual Workshop today!

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

75 YEARS RIMS *the* risk management society

contents

FEATURES

16 / 10 Tips for Developing an Effective ERM Program

Compiled from decades of challenges faced and lessons learned in risk management, these tips can help organizations create a successful enterprise risk management program.

20 / How to Overcome Cognitive Biases in Risk Management

By exploring eight of the most pervasive biases shaping ERM today, risk professionals can better develop pragmatic techniques to counter their effects and limit their impact on business decisions.

24 / How to Navigate the Volatile Tariff Landscape

As the Trump administration continues to implement sweeping global tariffs, companies need to engage in risk-based contingency planning to identify the potential impacts and manage the shocks.

30 / The Characteristics of Effective Risk Leaders

Focusing on these six practices can help risk professionals level up in their careers while also taking a more strategic and effective approach to risk management within their organizations.

WHAT'S INSIDE

2 Optimizing Your Enterprise Risk Management Strategy
These steps can help risk professionals enhance their organization's ERM approach and gain a strategic advantage.

5 Communicating Risks to the C-Suite
In times of uncertainty, the ability to communicate risk with clarity, balance and strategic foresight is critical.

8 Bridging the Gap Between Awareness and Action to Build Risk Resileince
Organizations not only need to build end-to-end risk and resilience capabilities, but also develop practical strategies to put those plans into action.

10 How Boards Can Navigate Geostrategic Risks
These considerations can help boards take an informed global perspective on opportunities and risks.

12 Building Operational Resilience in Third-Party Risk Managment
Building operational resilience requires a systematic framework for strengthening your TPRM program.

Shutterstock / Lightspring

RISK MANAGEMENT

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

CONTACT US

All submissions and letters should be sent to:

Morgan O'Rourke
Editor in Chief
Risk Management
morourke @ RIMS.org

T: (212) 655-5922

www.RMmagazine.com

Optimizing Your Enterprise Risk Management Strategy

by John Rogulak

In recent years, businesses have had to navigate a string of large-scale disruptions, underscoring that resilience is essential. As a result, enterprise risk management (ERM) is evolving from a compliance exercise into a strategic advantage. A structured, systematic approach to assessing and managing a broad range of strategic, operational, financial and compliance-related risks across an organization, ERM helps businesses stay ahead of volatility.

With rapidly advancing technologies, shifting regulatory environments and increasing interconnection among global markets, a proactive, risk-informed culture is critical. These seven considerations can help risk professionals enhance their organization's ERM approach:

CULTIVATE A RISK-INFORMED MINDSET ACROSS THE ORGANIZATION

At its core, ERM aims to build resilience and align risk with strategic growth. That begins with mindset, which involves understanding an organization's risk profile and aligning risk tolerance with strategic objectives.

A risk-informed mindset must start at the top and cascade through the entire organization. Corporate boards should engage in risk-based discussions to ensure organizational security and work with management teams to integrate ERM into organizational strategy. In turn, management should foster a risk-aware culture, educating employees about the importance of risk management and encouraging proactive risk identification.

UNDERSTAND THE ORGANIZATION'S RISK PROFILE

Effective ERM starts with the risk management team having a deep understanding of the organization's internal and external risk profile, supported by risk assessments that gather insights from a wide set of stakeholders. Often supported by audit committees, risk managers must conduct ongoing assessments that incorporate input from across the organization. This threat detection process

Shutterstock / JOURNEY STUDIO7

empowers the team to analyze and implement risk mitigation strategies that enable the organization to thrive.

It is essential that the risk management team work closely with the organization's board to ensure they are aware of the most consequential risks facing the organization, such as market trends, regulatory changes and supply chain disruptions. Understanding the operational threats and overall risk landscape will help ensure the board is making well-informed decisions that enhance resilience.

Risk managers should also familiarize the board with the risk management strategies already in place. This awareness ensures that board actions and decisions support ongoing risk mitigation efforts and create opportunities to strengthen the risk management team.

ALIGN RISK TOLERANCE AND APPETITE

Once the board and risk management team understand the risk profile, it is important to solidify the organization's risk tolerance and risk appetite. Before formulating an updated response plan, it is essential for the board and risk professionals to reach a consensus on the level of risk they are comfortable taking on to maintain desired performance levels.

It is equally important for other internal stakeholders to comprehend the agreed-upon risk tolerance and appetite. Although the board does not need to be involved in every decision, it is vital that the risk management team and other leaders are aware of the board's stance, enabling them to make informed strategic decisions that align with the established risk tolerance level.

These discussions should be approached as opportunities for organizational enhancement and alignment. Given that risk is defined as future uncertainty with both positive and negative potential outcomes, companies must manage both the upside and downside of risks. By reframing risks as opportunities for positive change rather than merely consequences to avoid, organizations can remain prepared to capitalize on organizational changes.

PLAN FOR BLACK SWAN RISKS

Traditional risk analysis typically relies on two criteria: the impact of a risk and the likelihood of its occurrence. During risk assessment, equal weight is often given to both factors, but this approach can be short-sighted and may ultimately hinder progress toward the organization's strategic objectives.

A structured, systematic approach to assessing and managing a broad range of strategic, operational, financial and compliance-related risks across an organization, ERM helps businesses stay ahead of volatility.

Assigning equal importance to impact and likelihood tends to minimize black swan events—rare occurrences with extreme consequences. Recent global crises have demonstrated that the improbable is possible, and black swans cannot be ignored. The COVID-19 pandemic and the 2024 CrowdStrike outage are examples of foreseeable yet unlikely events that significantly disrupted business operations. While many organizations had identified these events as possible risks, they under-prioritized preparation or mitigation due to the low likelihood assessment. That approach left organizations unprepared for these black swan events, which profoundly affected both internal and external stakeholders.

To effectively address potential black swan risks, risk managers must shift from probability-based thinking to impact-based planning, preparing for extreme outcomes even if their likelihood seems low. Resilient organizations develop contingency strategies that encompass the full risk environment—not just the most likely events.

ADOPT A COLLABORATIVE APPROACH TO RISK ASSESSMENT

Risk managers must understand the importance of conducting risk assessments for identifying, analyzing and prioritizing risks to avoid strategic missteps, missed opportunities and worst-case loss scenarios. However, traditional risk assessment methods often come with challenges in ensuring timely representation of all stakeholders and gathering meaningful, actionable data. Most risk assessments rely on manual methods like interviews and surveys to gather insights from various stakeholders and external sources. This process can be cumbersome and prone to errors, focusing mainly on threats while neglecting opportunities.

Collaborative methodologies and tools can address these challenges, enhance the risk assessment process, and enable organizations to proactively mitigate risks

and uncover growth opportunities. As risks become more interconnected, managing them in isolation is impractical. Traditional ERM methods often use impact and likelihood criteria, which provide a limited view and overlook risk tolerance and strategic goals. An improved collaborative approach offers a holistic perspective by leveraging historical data, industry benchmarks, continuous monitoring and communication. This approach involves stakeholders across the organization, which can enhance early detection of emerging risks and effective prioritization, boosting resilience and fostering a stronger risk culture.

LEVERAGE COLLABORATION TOOLS

Relying on traditional ERM methods to conduct a collaborative risk assessment that involves multiple stakeholders and up-to-date insights can be difficult, costly and time-consuming. Leveraging collaboration tools can help enhance an organization's approach to ERM.

Technology-based collaboration tools allow for quicker, more efficient risk assessments with higher-quality outputs and facilitate remote collaboration, allowing broader stakeholder inclusion and enriching risk identification with diverse perspectives. These tools can also capture risk information anonymously, encouraging diverse input and providing a voice to all stakeholders. Real-time collaboration automates repetitive tasks, which can enable teams to focus on outcomes and foster deeper discussions and better alignment on key risks.

DEVELOP AN ENHANCED ERM APPROACH

Enhanced risk assessments necessitate collaborative methodology and technology-enabled tools. Effectively leveraging collaborative tools can significantly enhance both the risk assessment process and the quality of the data it produces, enabling organizations to continuously plan for what is on the horizon.

Enhanced ERM can be broken into the following three phases:

1. Data collection: In this phase, the focus shifts from merely identifying risks to informing strategy. This involves questioning how the organization measures success and identifying significant roadblocks. Technology-enhanced assessments can leverage a risk universe tools that list multiple sector-relevant risks to broaden perspectives and gather richer data.

2. Risk analysis and prioritization: Collaboration software can help engage individuals, prioritize risks and build consensus quickly, reducing the traditional data collection period. The analysis and prioritization phase takes risk tolerance, management preparedness and risk velocity into consideration, emphasizing high-impact events and necessary responses.

3. Outcome and reporting: Technology-driven collaboration tools assess risk scenarios, foster stakeholder consensus and quantify impacts. These tools automate reporting, providing timely and insightful analysis that shapes response plans and guides strategic decisions.

Enterprise risk management is not about avoiding failure—it is about enabling, agility, insight and growth. By fostering a risk-aware culture and leveraging collaborative, tech-enabled tools, organizations can not only weather uncertainty but transform it into a strategic advantage. R

Shutterstock / Nichcha

John Rogula is the managing director of risk advisory at Baker Tilly.

Shutterstock / rudall30

Communicating Risk to the C-Suite

by Caldwell Hart

Modern risks are rarely isolated and never static. Geopolitical tensions, economic shifts and environmental disruptions now intersect with increasingly complex supply chains, placing growing demands on organizational agility and resilience. For example, among the most headline-grabbing risks are tariffs, which have recently been imposed, lifted or altered with little warning, often disrupting procurement and operations. Risk managers know that focusing on a single issue like this, no matter how urgent, can lead to strategic blind spots. Risk managers must help the C-suite see beyond headlines, assess risk in a broader context and avoid over-indexing. In times of uncertainty, the ability to communicate risk with clarity, balance and strategic foresight becomes one of the most critical responsibilities of the modern risk leader.

SEEING THE BIGGER PICTURE

With any risk, it is important to look at the bigger picture. Consider how the volatile nature of current U.S. trade policy has made tariffs an urgent concern. Shifts in import duties can quickly inflate costs, disrupt supplier relationships and force reactive adjustments to sourcing strategies. This presents a critical risk that demands detailed awareness and action, but there is danger in treating tariffs as a standalone risk rather than part of a wider ecosystem. A tariff change may drive companies to shift sourcing to alternate geographies. However, doing so may expose the company to new risks, such as reduced supplier quality, unfamiliar regulatory frameworks, logistics capacity and cybersecurity threats.

No risk exists in a vacuum, and messaging about risks should reflect that. It is essential to communicate with the C-suite in a way that highlights dependencies, not just singular disruptions. Senior executives have long relied on risk leaders for insight into external threats. However, increased expectations that companies respond immediately to global events can cause an organization to react before having all the information.

Executives are bombarded with information, and their natural instincts may be to act quickly. When tariffs dominate the news cycle, leadership may react by focusing solely on adjusting sourcing or renegotiating contracts. While urgency is understandable, single-risk responses may inadvertently introduce new vulnerabilities, increase costs and undermine long-term strategies.

This is why risk managers must communicate not just what the risks are but also provide the context by asking questions. For example: How likely is it that the risk

will escalate? What is the timeframe? What is the opportunity cost of reacting immediately? What other initiatives could be delayed or deprioritized? What opportunity does reacting immediately present? And most importantly, what combinations of factors are in play?

To support this kind of holistic, multidimensional thinking, risk professionals communicating with the board must focus on translating issues using clear, business-relevant language specific to the organization, and must take a balanced approach supported by facts.

BREAKING DOWN SILOS

To communicate risk effectively, risk managers need visibility and engagement across the organization. Though tariffs originate from governmental trade policy, their effects impact many departments. Risk professionals should proactively collaborate across departments to build a comprehensive view of risk and resulting impacts on corporate goals. For example, consider:

- Partnering with engineering and operations teams to understand how sourcing changes could impact design and manufacturing timelines
- Engaging IT and cybersecurity teams to assess potential vulnerabilities introduced by new supplier integrations
- Gathering input from finance to model cost increases, margin compression or currency exposure
- Consulting compliance and legal teams to evaluate the regulatory implications of shifting suppliers or expanding operations into new regions

Breaking down silos and synthesizing input from different business areas can help create a more comprehensive and accurate risk assessment for senior leadership and other stakeholders that is grounded in facts and operational reality. This also demonstrates to leadership that the risk team is embedded in strategic decision-making, not reacting in isolation. With this balanced approach, the organization can develop a comprehensive plan to address near- and long-term considerations.

Shutterstock / VisualBricks

Risk professionals communicating with the board must focus on translating issues using clear, business-relevant language specific to the organization, and must take a balanced approach supported by facts.

COMMUNICATING RISK WITH STRATEGIC CLARITY

Once a complete picture of risk is assembled, the next step is presenting it in a way that resonates with senior leadership. The objective is not to overwhelm the C-suite with detail, but to contextualize and prioritize risk so leaders can make swift, informed decisions, using the following key strategies:

1. Anchor Risk to Business Objectives

Always frame risks in terms of how they will affect growth, profitability, customer satisfaction and market reputation. For example: "If we react immediately to this tariff by shifting suppliers, we will increase short-term cost efficiency, but it could reduce our supplier diversity and increase exposure to labor compliance issues, undermining ESG commitments."

2. Use Visual Tools to Show Interdependencies

Risk heat maps, dashboards or spider charts can be powerful ways to display multiple risks and their interconnections. Instead of a long list of concerns, these visual tools show how different risks relate and where the most pressure points might form.

3. Present Trade-Offs, Not Just Threats

Every solution usually comes with a compromise. Strong C-suite communications should outline at least two scenarios, highlighting the preferred path and

alternatives. For example: "Delaying a supplier shift may cost more in the short term but allows time for quality assurance and cybersecurity reviews. Accelerating the move could avoid potential tariff exposure but increases operational risk." This approach positions risk managers as strategic advisers, not just problem-flaggers.

4. Balance Immediate Action with Long-Term Strategy

An organization's leaders are often looking for answers now. Risk managers must be able to defend both immediate responses and their alignment with long-term goals. Consider this example: "Our short-term mitigation for tariff increases is to absorb some of the cost, but we recommend a phased supplier transition plan over 12 months to ensure resilience and regulatory compliance in new regions." Providing a now-and-next plan builds credibility and keeps leadership grounded.

THE EVOLVING ROLE OF THE RISK MANAGER

Tariffs may be the headline risk of the moment, but tomorrow, it could be sanctions, climate events, supply chain labor laws, AI compliance or all of these simultaneously. Risk managers must guide senior leaders through today's dynamic landscape of interconnected, ever-changing threats with measured, clear communication rooted in strategic insight. By synthesizing cross-functional inputs and framing supply chain risks within the organization's broader goals, risk leaders can become indispensable partners to the C-suite—not only in time of crisis, but as a constant presence. R

Caldwell Hart is the principal of procurement and supply chain management at Avetta.

Shutterstock / Golden Dayz

Bridging the Gap Between Awareness and Action to Build Risk Resilience

by Joey Gyengo and Prasanna Govindankutty

Organizations are facing economic, technological and geopolitical disruptions at an unprecedented level, demanding more proactive strategies to manage risk. It is critical that organizations not only build end-to-end risk management and resilience capabilities, but that they also develop practical strategies for putting risk and resilience plans into action.

The *2025 KPMG Risk and Resiliency Survey*, which surveyed more than 200 C-suite leaders of large organizations, revealed a troubling disparity between organizational awareness of the urgent need to improve resilience and execution of the fast, agile and continuous risk management measures necessary to manage threats and disruptions that organizations are currently dealing with.

THE CURRENT STATE OF RISK AND RESILIENCE MANAGEMENT

As resilience is paramount to survival and success, bridging this gap should be a priority for executives in all industries. A good starting point is to assess what is working and what is not across risk and resilience strategies, structures, tools and capabilities.

In the KPMG survey, leaders acknowledged the importance of risk and resilience management, but many businesses lacked structured systems needed to address sudden, broad disruptions. Almost half of leaders (48%) said their organizations had a centralized struc-

ture managing risk and resilience, but only 17% had resilience plans that extend beyond critical processes.

In addition, the survey found:

- 26% of organizations had strong collaboration and a holistic, cross-functional view of risks
- 15% were heavily reliant on advanced analytics to identify, monitor and manage risks
- 41% expressed high confidence in their leadership's ability to effectively manage risk

These results suggest that many organizations lack the agility to cope with a dynamic risk landscape. Reactive risk management—focused on tracking specific risks, but without visibility to manage widespread risk impacts or ensure broad risk coverage—is ineffective at anticipating and responding to crises.

HOW TO BUILD A RESILIENT ENTERPRISE

Businesses need resilience strategies and capabilities that are tightly connected, gap-free, and able to adapt rapidly to change and keep pace with evolving threats. While every organization is unique, business leaders can take key steps to strengthen their organizations' resilience:

Start at the top with leadership buy-in. Successful risk and resilience management begins with full cooperation from top leadership, starting with building a strong understanding of the link between risk and resilience. Organizations with a consistent and uniform view of risk perform better in tracking emerging risks, experience fewer barriers, maintain more advanced capabilities and gain stronger confidence in the C-suite's understanding of business risks.

Centralize, integrate and collaborate. To ensure cohesive and well-informed decision-making, organizations need to avoid encapsulated processes and point solutions scattered across multiple business functions that do not talk to each other or that make it difficult to collaborate. A centralized and integrated approach can help organizations promote collaboration when identifying and managing risks.

Embed resilience into business strategy. Align and build risk management and supporting capabilities with the business strategy to achieve greater resilience. The survey indicated that leaders are starting to have the right conversations and ask the right questions, such as: What is most critical? What drives revenue? What would impact our reputation? What would shut us down? When resilience is embedded into the business strategy, it strengthens the organization's ability to quickly adapt in the face of adversity.

Utilize technology and tool sets for better outcomes. Specialized technologies such as governance, risk and compliance (GRC) platforms, artificial intelligence and advanced analytics can increase resilience and support a more robust approach to risk management. While two-thirds of organizations in the survey had mostly automated their processes, only 11% had achieved full automation.

Avoid a one-and-done approach. Organizations can foster a culture of resilience and continuous improvement that rewards accountability for risk-taking, clarity through specific policies and guidelines, and cross-stakeholder engagement in matters that impact the company's well-being.

Adopt ERM processes. Enterprise risk management (ERM) can make a critical difference in integrating risk management functions and enhancing an organization's resilience. By promoting collaboration among different functions, ERM ensures that risk and resilience strategies are robust, aligned and continuously improved.

Leverage external data sources for greater understanding. Integrate external data sources like market trends, industry benchmarks, government agencies, academia, consultancies and third-party data providers into your risk analysis procedures. This can help ensure that your risk perspectives are comprehensive and well-grounded.

Proper risk and resilience management is more critical than ever, yet many organizations struggle to translate recognition into action. Indeed, according to the survey, 72% of organizations face moderate or strong barriers to effectively managing risk. Bridging the gap requires a proactive, integrated approach that emphasizes leadership accountability, centralized frameworks and strategic collaboration. As threats continue to evolve, resilience must remain a continuous priority.

Joey Gyengo is the U.S. enterprise risk management leader and principal at KPMG LLP. **Prasanna Govindankutty** is the U.S. cyberrisk and GRC leader and principal at KPMG LLP.

Shutterstock / WhyFrame, Gorodenkoff, Mr. Virtual

How Boards Can Navigate Geostrategic Risks

by Robyn Bew

Many chief executives and board members have spent the majority of their careers in a business environment characterized by relatively open flows of trade, people and information as well as generally stable global alliances. However, the past five years have brought a series of sweeping changes to the international order that increasingly appear to be structural rather than cyclical. The risk landscape is more global, interconnected and fast-moving than ever before, which increases the importance of managing and mitigating those risks and being early to identify opportunities to secure a competitive edge.

In collaboration with the EY-Parthenon Geostrategic Business Group, the EY Center for Board Matters explored how leading boards are adapting their oversight activities to navigate a more complex, fragmented and uncertain international business climate. There have been dramatic changes in the way board members are addressing geostrategic risks and opportunities in just the past few years. For example, the EY-Parthenon's *Geostrategy in Practice* survey found that in 2025, 84% of organizations reported that their board of directors assessed the impact of political risk on the company's existing strategy compared to 40% in 2021.

The survey's findings point to three questions directors should consider:

1. Is the board staying sufficiently informed to help manage global macroeconomic, trade, regulatory and policy matters?

The biggest change in the survey results between 2021 and 2024 was the increase in directors who reported that their board regularly receives political risk briefings from external subject-matter experts, rising from just 16% in 2021 to 82% in 2025. The survey also revealed a large increase in the percentage of boards that regularly get briefings on these topics from company management.

However, directors should devote attention to the quality of the geopolitical information they receive, not just the quantity or frequency. Leading boards set expectations that the format and content of board reports will enable constructive dialogue during board meetings. Reports should be focused and forward-looking while featuring analysis of trends, patterns, implications and business impact and using easy-to-consume formats such as summaries, callouts, graphics, audio and video.

How those in the boardroom use the information is also critical. Directors repeatedly say that their number-one priority for improving the quality of board meetings is spending more time in open discussion and less time listening to management presentations. The best insights and analyses are useless if board members do not have an opportunity to discuss and debate their impact on strategy and long-term value creation.

2. Do existing transaction and alliance plans reflect new geostrategic realities? Joint ventures, partnerships, spinoffs and acquisitions can help catalyze innovation, growth and competitive advantage. The EY-Parthenon survey found a dramatic uptick in the percentage of directors who say their board regularly incorporates political risk considerations into areas such as mergers and acquisitions and market entry, surging to 77% in 2025 from 25% four years earlier. This is happening via strategic portfolio reviews, constructive challenges of deal assumptions and close monitoring of post-deal integration and change management. Board members should consider the following questions:

- How are international developments—including taxes, trade, tariffs, immigration policy and consumer preferences—affecting our portfolio strategy and decisions about deployment of capital?
- How is board oversight enabling a future-back view of how the company's competitive landscape might change over the long term given emerging trends, and how are related discussions informing the company's transaction strategy?
- What are the core assumptions that must be true for a deal to succeed and what is management's plan if the facts on the ground change?
- How can the board and management use the successes and failures of past deals to mitigate common missteps in processes related to transactions or alliances?

3. Is current scenario planning fit for purpose? Scenario planning is an area of improvement for boards and senior management teams to consider as it was the geostrategy oversight activity survey respondents cited least frequently. To address that deficiency, they can start with a conversation about risk appetite: How well aligned are the board and senior leadership on what the appropriate levels of risk to take are with respect to areas like global mergers and acquisitions, joint ventures and partnerships, supply chain, cybersecurity, and talent?

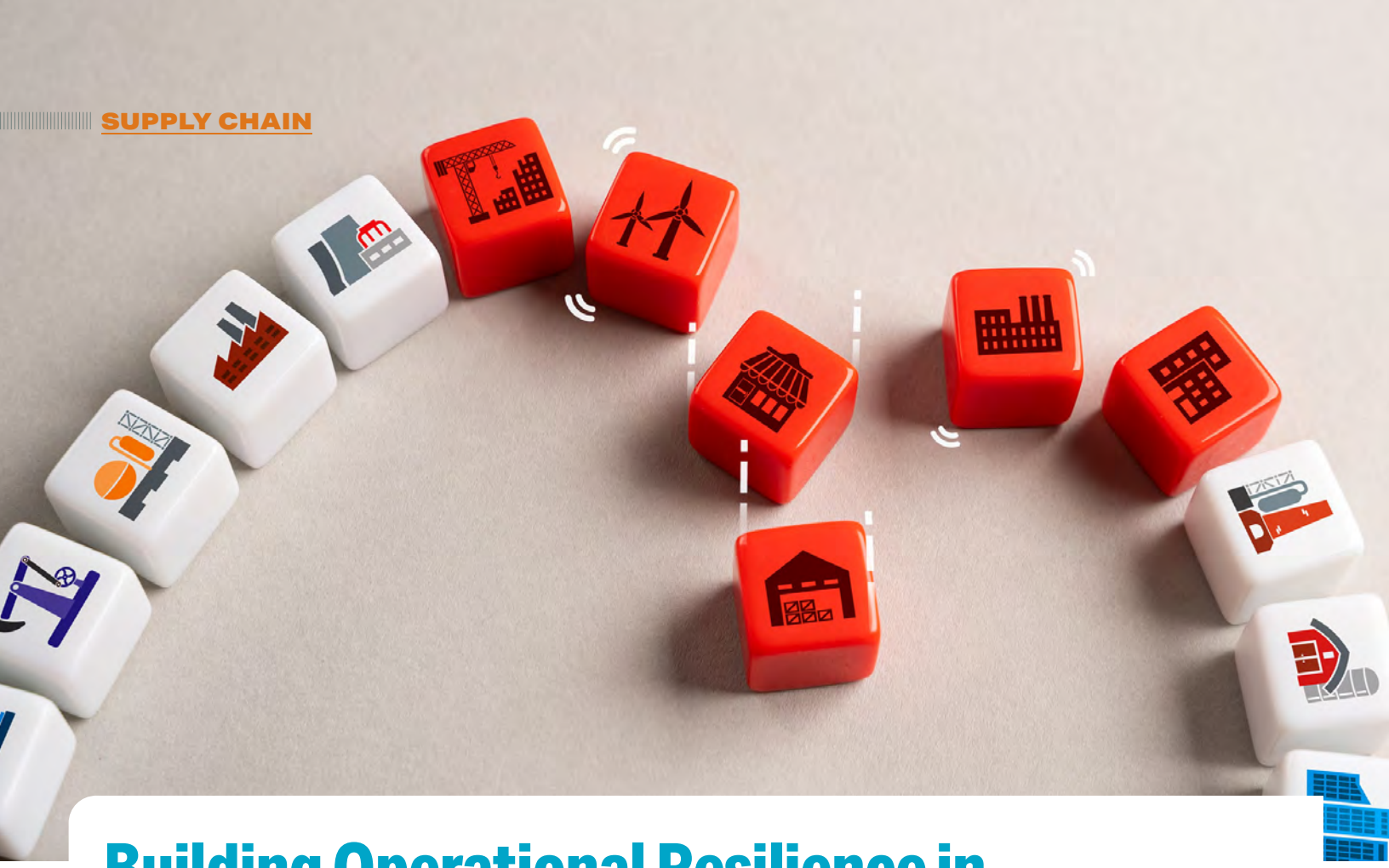
Geopolitical fragmentation is combining with the momentum of megatrends such as technology transformation, climate change and demographic shifts to create a baseline level of volatility and uncertainty for businesses.

From there, the board can explore questions such as: Do management's scenarios for either downside risk (existential threat to the company) or upside opportunity (significant outperformance) consider a broad enough range of outcomes? What metrics provide early-warning indicators that a negative or positive scenario could be materializing and what would be the trigger points for deciding to act?

GOVERNING AMID ONGOING VOLATILITY AND UNCERTAINTY

While the exact shape of the international order in 2026 and 2027 may be difficult to predict, geopolitical fragmentation is combining with the momentum of megatrends such as technology transformation, climate change and demographic shifts to create a baseline level of volatility and uncertainty for businesses that seems likely to continue. Directors need to take these new geostrategic conditions into account by integrating an informed global perspective on opportunities and risks into the work of the board. R

Robyn Bew is the director for EY Americas Center for Board Matters at Ernst & Young LLP.



Shutterstock / Andrii Yalanskyi

Building Operational Resilience in Third-Party Risk Management

by Ryan Patrick

Third-party risk management (TPRM) has reached a critical inflection point. Traditional approaches focused on compliance assessments and security questionnaires are proving insufficient for today's interconnected business environment. From ransomware attacks to supply chain failures and cloud outages, high-profile disruptions have exposed a fundamental gap: Organizations are measuring vendor security, but not vendor resilience.

When a single vendor goes down, the ripple effects can be catastrophic for every business that relies on them. This is forcing organizations to rethink their approach to TPRM and expand their focus from reactive risk assessments and compliance checkboxes to proactive resilience and business continuity. It is not enough to ask if a vendor is secure—the better question is if an organization can withstand the operational impact if that vendor is taken offline tomorrow.

Most TPRM programs excel at evaluating whether vendors protect data but struggle to assess whether they can maintain operations under pressure. A vendor might have pristine SOC 2 reports and ISO certifications yet lack the recovery capabilities to withstand a major disruption. This gap becomes critical when you consider that modern businesses often depend on dozens of third-party services for core operations.

The Change Healthcare breach illustrated this perfectly. As a payment intermediary handling billions in medical claims, the company's operational failure affected its business as well as thousands of healthcare providers who could not process payments, verify insurance or fill prescriptions. The compliance frameworks

that validated Change Healthcare's security posture had not captured its role as a critical dependency for an entire industry.

A FRAMEWORK FOR RESILIENT TPRM

Building operational resilience requires a systematic approach that goes beyond traditional risk assessments. The following is a comprehensive framework for strengthening your TPRM program:

1. Map Critical Dependencies and Business Impact

Start with a thorough dependency mapping exercise that identifies which vendors you use and how critical they are to your operations. Creating a dependency matrix can help simplify this process. Categorize vendors by asking:

- What business processes would halt if this vendor went offline?
- How difficult would it be to replace this vendor or implement workarounds?
- How would a vendor outage affect your customers, partners or stakeholders?

Business impact scores can be based on revenue loss, operational disruption and regulatory exposure. This helps prioritize where to focus your resilience efforts. An organization should also trace and document how a vendor failure would impact various areas of the business. Often, the most critical dependencies are not obvious until you map the connections.

2. Expand Risk Assessments Beyond Security Controls

When evaluating third parties, go beyond cybersecurity policies. Ask about their disaster recovery plans, recovery time objectives and recovery point objectives. Additionally, ask them to demonstrate backup systems and data replication strategies, incident response procedures and escalation protocols and business continuity testing frequency and results.

If a vendor is unwilling or unable to provide this information, that is a red flag. Operational transparency is now as important as technical security and vendors should be willing and able to demonstrate their monitoring capabilities, communication protocols during incidents and historical performance during disruptions.

3. Strengthen Internal Contingency Planning

Organizations cannot control whether a vendor experiences problems, but they can control their response. The most resilient organizations prepare for vendor failures with the same rigor they apply to other business continuity scenarios. Each critical vendor needs a vendor-specific contingency plan, including pre-identified alternative providers with which you have established relationships, manual workarounds for key automated processes and clear decision criteria for when to activate backup plans.

The goal is to build operational buffers before they are needed, which means maintaining relationships with secondary vendors, keeping backup systems ready for activation and training staff on emergency procedures. Organizations should also account for the hidden costs of vendor disruptions including overtime, expedited services, revenue loss and customer retention efforts. The key is not leaving it up to contingencies that take weeks to implement or leave an organization scrambling for emergency funds in the middle of a crisis.

4. Implement Dynamic Risk Monitoring

Annual risk assessments might be inadequate in today's fast-moving threat landscape. Modern TPRM requires continuous monitoring that spots problems before they become crises. The best monitoring systems help organizations understand patterns, predict issues and continuously refine vendor risk assessments based on real-world performance.

Consider deploying comprehensive monitoring that tracks both security and operational health indicators, including automated alerts for vendor security incidents and performance degradation, financial stability monitoring through credit ratings and newsfeeds, and social media and industry intelligence for early warning signs.

If an organization is just getting started with a TPRM framework, it should focus on calibrating alert systems to minimize noise while maximizing signal. Too many false alarms and a team becomes numb to warnings; too few and a team is caught off guard when genuine threats emerge. The sooner an organization knows a vendor is compromised, the faster it can activate contingency plans.

5. Foster Collaborative Vendor Relationships

The strongest vendor relationships are built on shared responsibility for resilience rather than one-sided auditing. Treat critical vendors as strategic partners invested in mutual success and establish transparent communication protocols that define the method and timeframe for incident notification, what information they will provide during disruptions and clear escalation paths for critical issues.

An effective way to strengthen a vendor

relationship is to invite them to engage in joint resilience planning through regular business continuity exercises, shared threat intelligence and co-developed incident response procedures. When vendors understand how their failures impact the business they work with, they are more likely to invest in preventing those failures. Organizations can also design service-level agreements that reward resilience, preferred vendor status for operational excellence and financial penalties for avoidable disruptions.

6. Build Organizational Resilience Capabilities

Internal capabilities determine whether contingency plans succeed or fail under pressure. The most prepared organizations invest in people, processes and governance structures that can execute effectively during vendor crises.

Team members from the IT, legal, business continuity and communications departments should be part of an active cross-functional response team. The key here is having the right people on the team. They need to work together regularly and understand each other's capabilities before a crisis hits. Realistic exercises that go beyond theoretical tabletop discussions can include scenario-based drills that simulate actual vendor failures, technical exercises that test backup system activation and communication drills for managing stakeholder expectations.

Every organization needs clear governance structures that define decision-making authority during crises. This includes who can authorize expensive backup systems, approve emergency contracts and speak for the organization during outages. Without clear governance, vendor crises often become organizational crises.

The organizations that adapt to current TPRM needs will be the ones that thrive in an increasingly interconnected and disruption-prone business environment. Those that cling to compliance-only approaches risk being caught unprepared when the next major vendor incident occurs.

Ryan Patrick is the vice president of market research and adoption at HITRUST.

MEMBERS SAVE UP TO 40% ON THE RIMS-CRMP APPLICATION

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**

75 YEARS RIMS
the risk management society®

10 Tips for Developing an Effective ERM Program

by Michael J. Cawley

Developing an enterprise risk management (ERM) program can be a difficult task, even for experienced risk professionals. While there is no one-size-fits-all approach, the following tips—compiled from decades of challenges faced and lessons learned in risk management—can help organizations achieve their own ERM success.

1. Create a Succinct ERM Mission Statement

As a vital first step toward the establishment of a robust and meaningful ERM program, all companies should consider developing and memorializing a mission statement that explains the primary purpose of ERM. The statement should combine strategy with tactical execution by focusing on actionability instead of empty buzzwords or jargon, and be succinct to encourage understanding, consensus and transparency.

Essentially, the mission statement must tie together the "what" and the "why" of ERM. For example: "Enterprise risk management is the process for identifying, assessing, mitigating and monitoring all enterprise-wide risks that might impair the company's ability to achieve its strategic business objectives."

2. Establish a Risk Management Framework

Expanding upon the ERM mission statement, risk professionals should formulate another program cornerstone: the risk management framework (RMF). This is the authoritative manual that "sells" and guides your ERM program.

There are three key distinct components to every successful RMF. In the initial section, set the context for ERM. To get there, take stock of your company's identity and explain why ERM can make a tangible difference by asking the following questions: What does your company do and what are its unique business characteristics and drivers of success? What is the connection to, and reliance upon, risk management? How does the discipline of ERM potentially impact the company's high-level business goals, such as earnings performance, capital preservation, liquidity maintenance and reputation protection?

The second section of the RMF establishes the foundational elements of ERM by detailing the company's overall cultural model and spelling out the company's identity, what it recognizes and rewards, and the ethical behaviors it expects. Here, the company should also establish the risk governance structure with roles and responsibilities delineated by line of defense. At a very high level, this second section of the RMF should also speak to the concepts of risk appetite and tolerance, the latter reflecting specific pre-defined threshold where appetite is exceeded, triggering notification, assessment and/or corrective action.

The third section of the RMF addresses the tactical execution of ERM. This process comprises the following elements: 1) identifying risk on an iterative basis, with the net result being your universe of exposures; 2) assessing risk in a consistent and transparent manner, particularly focusing on severity and likelihood; 3) mitigating inherent risk severity and likelihood to an acceptable residual level through well-defined controls; and 4) monitoring risk on an ongoing basis, pinpointing prominent metrics, such as key risk indicators (KRIs), and disseminating reports for both internal and external use.

3. Connect Your Overall Corporate Culture to Risk Management

Risk culture represents the shared understanding and behavioral attitudes of the company's employees toward risk-taking and comprises key pillars like governance, training, risk-aligned performance and business conduct. How does your risk culture connect with a company's overall culture that dictates conducting business with integrity and ethics at all times?

Simply put, a company should strive to cultivate a high-performing environment that is inclusive and equitable at the same time. All employees should feel empowered to do their best and contribute to their fullest potential to advance and thrive in their careers. The overall culture should guide day-to-day decisions and link brand identity with behaviors that are both expected and rewarded.

4. Pinpoint Your Risk Universe

When defining a risk universe, the key point is straightforward: Do not miss a single risk. It is also important to allow flexibility such that emerging risks can be readily incorporated, and to sub-categorize or break down the overall universe in a way that makes sense and makes it digestible.

For instance, you might want to consider establishing three core categories at the outset—financial, operational and strategic—as these appear consistently across all risk registers, no matter what industry the company represents. Then you can construct a customized core risk category that reflects

AdobeStock / Golden Sikorka

Shutterstock / Anton Vierietin

the source of your revenue streams (e.g., retail, manufacturing, construction, insurance).

5. Institutionalize a Formal, Automated Risk Register

Full implementation and consistent use of an automated risk register tool is vital to ERM success. Mere spreadsheets will not cut it. The ideal risk register should focus on a small number of key risk attributes (causes, consequences, controls and key risk indicators) and select metrics (severity and likelihood, as well as direction and velocity) that will enable risk assessment and prioritization. It is important to appoint one risk owner per risk to establish accountability from the outset.

6. Continually Hone Your Risk Rating Scales

Establishing understandable and transparent severity and likelihood rating scales is crucial to foster both risk governance and risk culture. Keep in mind that simple descriptive identifiers like "high" or "rare" can expose you to potential misinterpretation. Instead, be specific when defining severity and likelihood and modify the definitions as needed.

For example, severity determination can be predicated on a number of different indicators, such as financial impact, brand/reputation, regulatory or strategic. Use whatever indicator lends itself to the risk in question and best resonates with the risk owner.

In terms of likelihood, rating scales should not measure the chance of incurring just any risk event. Rather, it should address the possibility of a significant event as defined in the severity table that you formulate. An "almost certain" rating might anticipate a significant event once every year, while a "rare" rating might project a significant event only once every 50 years.

7. Establish Material Risk Policies

Risk policies should articulate a company's general approach to the identification and management of material risks. Policies are

high-level approaches to decision-making, include significant discretion, and are often delineated in qualitative terms rather than qualitative measures.

As a rough measure, there should be policies for a dozen or so material risks in your universe. Each risk policy should generally address: 1) the definition of the risk policy in question; 2) the goal of the risk policy; 3) controls that mitigate the risk, itemized by line of defense; 4) roles and responsibilities to manage the risk; 5) risk appetite for the risk in question; and 6) specific risk tolerances and escalation provisions in the event of exceedance.

8. Actively Promote the Embedded Risk Governance Structure

ERM should never be considered a separate service function. Rather, it should be looked at as a discipline consciously embedded in critical decision-making processes throughout the organization. Primary ownership for the daily execution of risk management rests with the business unit, with support from risk-related functions like ERM, compliance or internal audit, as well as risk-related boards and committees.

Risk governance structure is best portrayed in the three lines of defense model, where day-to-day management, control, oversight and independent assurance of risk are assigned to the following groups:

- **First line:** business units and supporting functions
- **Second line:** all groups responsible for ongoing monitoring and challenging of the design and operation of controls in the first line
- **Third line:** entities responsible for independent assurance over the management of risks, including challenging both the first and second lines

9. Set Appetite and Tolerances for All Key Risks

Risk appetite represents the general willingness to assume risk and, in turn, to expose the company and its capital to risk of loss. The establishment and enforcement of consistent, transparent and expected behaviors around risk appetite, conveyed through appetite statements and guidelines, is crucial to the risk management framework.

Drilling down deeper, risk tolerance reflects the specific pre-defined thresholds that exceed the appetite for a specific risk, triggering notification, assessment and/or potential corrective action by management. Key risk indicators (KRIs) are metrics that provide a way to quantify and monitor each risk. Think of them as change-related metrics that act as an early-warning system to help companies effectively monitor, manage and mitigate risks.

ERM should never be considered a separate service-function. Rather, it should be looked at as a discipline consciously embedded in critical decision-making processes throughout the organization.

10. Connect ERM with Other Risk-Related Disciplines

Once you construct and adhere to a robust risk management framework, there is no risk-related issue that cannot be confronted head-on. Consider the following risk-related areas:

- **Governance, risk and compliance (GRC):** This is a subcategory of your risk universe that simply slices and dices a smaller body of risks in a slightly different fashion.
- **Environmental, social and governance (ESG):** This is a mixture of operational (e.g., corporate governance) and strategic (e.g., climate risk) exposures, as well as the precepts from your overall cultural model described in the foundational section of your RMF.
- **Diversity, equity, and inclusion (DEI):** DEI initiatives are undeniably risk-related in nature and, like ESG, can be viewed through the prism of both the risk register (e.g., operational risks like human resources, talent management/retention and compliance) and, even more importantly, foundational elements contained in your RMF like ethics, culture and governance.

Whether the risk-related challenges are actual risks within your risk universe or principles addressed within your risk management framework, applying the discipline of ERM will still work to address the wide range of risks facing your organization. R

Michael J. Cawley is a risk management executive with more than 35 years of experience in the strategic and tactical elements of corporate enterprise risk management. He currently serves as a subject matter expert in an advisory role on ERM best practices for GRC software provider DoubleCheck.

How to Overcome Cognitive Biases in Risk Management

by Shreen Williams, Jason Rosenberg and Lisanne Sison

Risk professionals often take comfort in frameworks such as COSO ERM and ISO 31000 because they provide structure, discipline and a sense of order for organizations and their assurance capabilities. Regardless of the framework or the level of structure it may provide, there is one component that cannot be removed from the risk management process: human bias.

Biases are shortcuts in our thinking, helping us make quick decisions. Unfortunately, those decisions are not always the right ones. While biases may help us make faster decisions in times of uncertainty, they can also distort judgment. In high-stakes environments like critical business decision-making, even the slightest distortions can lead to strategic blind spots, wasted resources or surprises that have a severe impact.

Biases can show up at any stage of the ERM process lifecycle, from process design to risk identification and assessment to risk monitoring and reporting. Cognitive biases can appear in many forms, including boards choosing complicated solutions that look impressive, leaders explaining away mistakes and placing the blame on others, or teams of people going along with the group rather than speaking up to provide their own perspective.

It is not enough to simply be aware that biases exist throughout risk management processes. The real challenge for risk leaders is to proactively identify biases and develop mitigation strategies to minimize biased decision-making and support risk-informed decisions. Eight of the most pervasive biases shaping ERM today are complexity, innovation, self-servicing, overconfidence, anchoring, confirmation, framing and groupthink. By exploring these biases and the scenarios in which they manifest, risk professionals can better develop pragmatic techniques to counter their effects and limit their impact on business decisions.

When Complexity and Innovation Become a Crutch

Consider a hypothetical scenario: A company's board of directors decides to hire an external risk management consultant to evolve its capabilities and maturity level. The consultant completes the engagement and delivers a complex, jargon-filled, COSO-aligned framework with multiple taxonomies and negligible practical advice or resources to help the company implement the consultant's recommendations and ensure adoption from its internal stakeholders. Risk identification stalls because the framework is far too complicated for frontline employees to apply. The assumption is that

To learn more, check out the session **"Beating the Bias: Exposing and Combating Cognitive Biases in ERM"** with Shreen Williams at the 2025 RIMS ERM Conference.

Shutterstock / Andrii Yalanskyi

complexity is automatically better. This is **complexity bias** at work.

Complexity bias leads organizations to favor overly complicated solutions over pragmatic solutions. This bias is often accompanied by **innovation bias**, in which the newest version of a framework like COSO ERM is perceived as inherently superior, regardless of whether it drives actual improvements to existing capabilities.

These biases can have significant impact on risk governance. Making things too complicated can confuse frontline employees, delay progress and give stakeholders a false impression that their risk management capabilities are more advanced than they actually are. By making frameworks unusable for frontline teams, these biases can overcomplicate governance, undermine risk identification, and make it more difficult to establish risk frameworks and structures.

To overcome complexity and innovation biases, keep it simple. In risk governance discussions, ask yourself: Could I explain this framework to a new employee in less than two minutes? If the answer is no, it is too complicated, and complexity bias may be in play. Address the bias by trimming the extras and focusing on what really matters. Specifically, summarize risk governance structures and frameworks into one-page resource documents. Then, check with risk champions situated throughout the organization's ecosystem to validate whether the documents are digestible and accessible enough.

Falling Into the Self-Serving Trap

Imagine a company that is launching a new product. If it succeeds, leaders credit their foresight. If it fails, they blame regulators or "unforeseen" market shifts. After-action reports are shallow and lessons learned are rarely integrated into the ERM process. This is **self-serving bias**—attributing wins to ourselves and losses to external factors.

In strategy discussions, self-serving bias can lead to selective storytelling. Leaders may take too much credit for successes and downplay outside factors. This creates a false sense of confidence and prevents the company from learning from its mistakes, ultimately weakening the organization's overall strategy and future decision-making processes.

Overconfidence bias amplifies this problem. Decision-makers often overestimate their predictive abilities, underestimate downside risks and allocate resources based on optimism rather than balanced analysis of objective data. For example, a CFO may project best-case market growth while ignoring signals of regulatory headwinds.

Self-serving bias makes it more difficult to manage the ERM process. Strategic choices ultimately become management actions, including resource allocation, performance review and lessons learned. This is where self-serving attributions distort accountability and prevent organizations from integrating failures back into their risk programs.

To combat this bias, pair every major decision and postmortem review with an independent, objective challenger who is empowered to poke holes—not rubber-stamp—the narrative. This objective challenger could be a dissenting board member, an activist shareholder or an external advisor. Require teams to document both "management-controlled factors" and "external factors" before closing reviews to help ensure balance and accountability. The goal is not to obstruct or criticize, but to achieve objectivity to identify opportunities for improvement.

Anchoring Too Strongly on First Impressions

During a risk assessment, the first concept or idea mentioned can often "anchor" the rest of the discussion, even if it is arbitrary. For example, imagine a company holds an executive team risk workshop to address concerns of a potential cyber disruption event. The CISO tells the group that there is a 25% probability of a cyber disruption event materializing. Despite objective evidence showing the likelihood is actually higher, the number arbitrarily introduced then sets the tone for discussions. This is **anchoring bias**.

Anchoring bias frequently occurs in risk assessment workshops and budget allocation meetings. Once an initial anchor is set, it is tough for participants to move beyond it, even when better data becomes available. Anchoring bias can complicate risk assessments where risks are evaluated and scored as initial anchors can distort probability and impact judgments.

To prevent anchoring bias when facilitating workshops and meetings, consider sending all participants pre-reads that provide insights into the process and specific risks that will be evaluated or discussed. Use structured materials that require anonymous input from multiple perspectives like finance, operations and legal. Also make sure to calibrate results in validation sessions to reduce reliance on the first number put on the table.

Seeing What We Want to See

Consider a company where the chief risk officer reviews quarterly risk dashboards. Most indicators show stability, so they ignore a dissenting data set suggesting an emerging third-party vulnerability because it conflicts with their preferred narrative. This is **confirmation bias**—favoring information that supports what we already believe.

Confirmation bias is especially prevalent in situations where no consideration is given to alternative data and information, regardless of source or availability. Left unchecked, confirmation bias blinds risk management teams to new threats. It perpetuates outdated risk registers, discourages escalation and can leave organizations more vulnerable to severe risks. Confirmation bias interferes with risk monitoring where data and metrics are tracked. When organizations dismiss contradictory signals, they fail to detect changes in exposures or emerging risks.

To avoid confirmation bias, do not just look for evidence that supports your individual perspective. Instead, look for what might

prove it wrong. Rotate teams that are assigned to challenge attitudes and assumptions. They should act as adversaries to uncover blind spots in your organization's defenses and challenge the efficacy of your organization's internal control mechanisms. If your organization has an internal audit function, that team could also be well positioned to provide this insight. In every decision-making discussion, require leadership to provide at least one fact or example that challenges the current thinking, and review at least one opposing fact or example during each meeting.

Framing the Same Data for Different Decisions

After conducting a risk assessment, imagine a company's CISO reports to its board of directors that its system uptime is 95%. The board of directors and company leadership feel the targeted system uptime is adequate and use that data to reduce resource allocations for the company's IT business function.

Alternatively, the CISO could report to the board that their system downtime is 18 days a year. As a result, the board of directors and the company's leadership demand urgent resource allocations for the IT business function.

Though they may both be accurate numbers, a system uptime of 95% resonates more positively with the company's decision-makers than 18 days of downtime per year. This bias is known as the **framing effect**, where the same data can change perceptions and decisions when simply packaged and presented differently.

Framing bias affects how leaders interpret the same data. Positive frames typically encourage risk-taking and negative frames push toward risk aversion. As the way data is presented often directly impacts the choices leaders make, shifts in framing can shape multimillion-dollar investment decisions.

Avoid framing bias by standardizing dashboards and using neutral language in reports to reduce unconscious conclusions and present risk information in a way that showcases both upside and downside. Encourage decision-makers to reflect on the data before reaching a conclusion.

Betting Too Much on Gut Feeling

Consider another company where leadership is confident that their cloud migration will be seamless because their team has successfully executed projects before. They allocate minimal contingency funding, only to encounter months of delays and unexpected security gaps. This is **overconfidence bias** undermining resilience.

Overconfidence bias leads organizations to underestimate complexity, dismiss early warnings, over-rely on prior successes and overcommit to ambitious timelines. In risk assessments, this often leads to unrealistically optimistic scores, directly impacting how organizations allocate resources, establish timelines and execute risk responses.

To counter overconfidence bias, conduct premortems before all major initiatives, pretending that they have already failed and then working backwards to ask why. This "what could go wrong?" exercise helps uncover blind spots and hidden risks before decisions are locked in. Executive sponsors for the initiative should be able to explain why it could fail. Track variances between forecasted versus actual project outcomes to recalibrate future assumptions and allocate appropriate resources.

Favoring Consensus Over Candor

Boards often pride themselves on consensus, but too much harmony can easily hide both upside and downside risk. Consider a company where board meeting discussions often grow tense, but if the CEO confidently asserts their perspective, dissenting leaders hesitate to challenge the CEO or present their opposing perspective. Instead, they nod in agreement with the rest of the collective group to avoid "rocking the boat." Decisions are unanimous, and critical risk exposures are ignored. This is **groupthink**—the preference for consensus over candor.

Groupthink erodes the quality of reporting and oversight. It silences minority opinions, narrows perspective, and prevents boards from fulfilling their role as stewards of diverse stakeholder interests. Groupthink complicates the risk reporting process, where risk information is escalated to executives and boards. Suppressing dissent in reporting weakens oversight and masks exposures.

To overcome groupthink, adopt a formal "speak up" practice that encourages internal stakeholders at every level to speak freely, without any fear of retaliation or retribution. Implement a process for structured dissent, requiring a round of "what are we missing?" at every meeting. Allow anonymous submissions for alternative viewpoints and present them in future meetings to normalize candor and dissent. Embed psychological safety by rewarding dissent, not penalizing it.

The Human Side of ERM

Leaders who can combat bias in real time can help position their organization ahead of its peers and competitors. Frameworks, dashboards and internal controls are essential, but they cannot eliminate the most unpredictable variable in any ERM program: people. Biases creep into strategy discussions, risk assessments and board reports, often without anyone realizing it.

Human biases will never disappear, so risk leaders must embed bias-awareness into every stage of the ERM process lifecycle, not as an academic exercise, but as a daily discipline. Start small by simplifying frameworks, running premortems, rotating teams assigned to challenge perspectives and assumptions, and normalizing and rewarding dissent. Over time, these practices can help create positive risk cultures, healthier governance and more effective risk oversight. R

Shreen Williams is founder and CEO of Risky Business SW, LLC. **Jason Rosenberg** is senior director of risk and resiliency at Autodesk. **Lisanne Sison** is managing director of ERM at Gallagher.


IMPORT
TARIFFS

HOW TO NAVIGATE THE VOLATILE TARIFF LANDSCAPE

by Neil Hodge

For the past few decades, the prospect of a trade war triggered by tariffs and other protectionist policies had never posed a serious risk to companies, but times have changed. With the Trump administration issuing wildly varying directives and threats to impose or increase tariffs on dozens of countries, markets have been thrown into tumult, causing far-reaching complications and added costs for both businesses and consumers.

Many companies will face a wide range of impacts as soon as the tariffs take effect. Indeed, even the threat of tariffs and the climate of uncertainty have had significant material effects on businesses worldwide. One of the most obvious concerns is cost increases, with many companies currently scrambling to determine how to pass the additional burden on to suppliers and customers without losing or alienating either one. Another risk is reduced overseas supply options and the possibility that, if suppliers in low-cost countries are cut off from doing the same level of business in the markets in which a company operates, they could end up supplying the competition.

Indeed, the complexity of global supply chains makes it difficult for companies

Shutterstock / Tasnim911

to estimate their indirect exposure to tariffs if lower-tier suppliers are subject to them too. Companies will also need to perform more due diligence to determine whether existing suppliers will be subject to tariffs and potential tariffs that may apply to any new suppliers they onboard.

Experts believe companies should engage in risk-based contingency planning as soon as possible to identify the potential impacts and manage the shocks that tariffs could cause. With such a strategic approach, a business that adapts quickly can use the threat of tariffs to refine its strategies, rethink and reinforce its supply chains, and explore new markets and opportunities.

"Forward-thinking companies have been preparing for tariffs long before the U.S. election and continue to refine strategies to mitigate or capitalize on them," said Tyler Higgins, managing director at management and technology consulting firm AArete. "Businesses that integrate risk assessment into supply chain, procurement and pricing strategies will navigate tariffs more successfully than those reacting to policy changes."

The Importance of Contract Management

The imposition of new tariffs can be disruptive as well as expensive. After the initial reaction to stockpile as many products and materials as possible before the rules take effect, the easiest short-term solution is for companies to try to come to an agreement with their existing suppliers on a way to split any additional costs they incur going forward. In the long term, companies may want to exercise their specific rights within existing supplier contracts to account for tariff-related cost increases or insert more favorable terms for themselves in future contracts to mitigate financial risks. It may also be useful for companies to review termination and renegotiation clauses so that they can switch suppliers if tariffs make current sourcing strategies unsustainable.

"Contracts are one of the most powerful assets businesses can leverage," said Bernadette Bulacan, chief evangelist at contract management software vendor Icertis. Contracts should be the first resort for companies to fall back on, especially as "finding new suppliers and negotiating or renegotiating deals causes delays and leads to increased logistical costs and financial penalties," she said.

According to Heewan Noh, associate at law firm Huth Reynolds, several types of contractual provisions may prove useful. For example, fixed-price contracts typically assign cost risk to the seller. Suppliers cannot unilaterally demand price adjustments if tariffs increase their costs unless the contract allows cost-sharing mechanisms.

Similarly, some contracts tie prices to commodity indexes, mitigating the impact of sudden market changes. An indexed pricing structure may provide protection if a supplier anticipates tariff risks. So-called "incoterms" can also work well. These international trade terms define which party is responsible for tariffs, duties and transportation costs. Some industries prone to extended supply chains, such as the automotive sector, rely on these kinds of contracts precisely because they are a useful starting point for establishing tariff responsibility. For example, they may specify that the seller covers export costs while the buyer covers import costs.

Companies should use supplier contracts that explicitly specify which party is the "importer of record" as it will then be legally responsible for handling all importing requirements, including tariffs and the payment of customs duties, Noh said. Contracts should clearly define which party is responsible for tariff-related expenses, eliminating ambiguity.

Companies can also structure cost-sharing arrangements, where one party initially pays the tariffs but later receives full or partial reimbursement from the counterparty. Furthermore, contracts can include automatic renegotiation clauses that require the parties to revisit pricing if new tariffs, duties or other government-imposed charges are introduced post-execution. Companies can also include price adjustment rights in quotations or quote updates. This approach allows for pricing flexibility to account for sudden tariff increases, avoiding reliance on force majeure or commercial impracticability defenses, which courts often reject in tariff-related disputes.

Companies often believe that clauses like force majeure or commercial impracticability may offer opportunities for renegotiation or relief if substantial tariff changes occur. Both serve as defenses to contractual performance, meaning that the affected party is not considered in breach for failing to fulfill its obligations if a qualifying event renders performance impossible or impracticable.

"Businesses that integrate risk assessment into supply chain, procurement and pricing strategies will navigate tariffs more successfully than those reacting to policy changes."

However, these legal doctrines do not inherently provide a means for securing price increases and, as many companies found with the COVID-19 pandemic, they do not always offer the level of protection companies desire. While suppliers often invoke them in commercial negotiations to justify price adjustments, courts around the world have generally been unwilling to allow companies to withdraw from contractual commitments solely due to higher costs, whether from tariffs or any other factor.

Supply Chain Diversification and Tariff Engineering

Besides tightening up and enforcing contract terms, there are a range of other options companies should consider. High on the list is supply chain diversification. Depending on the sector they are in, some companies are more highly exposed to the threat of tariffs than others, which may necessitate immediate changes to offset any financial impact. To counter that risk, companies should assess whether they can shift sourcing to suppliers in countries with lower or no tariffs, including options like nearshoring, reshoring or "friend shoring," which is when organizations select partners in countries that are geographically closer and/or are members of the same trade bloc. Companies could also consider sourcing materials and components from multiple countries to reduce reliance on a single source that may be subject to tariffs. For this to work effectively, however, it will require thorough mapping of supply chains to find out where tier 2, tier 3 and lower-tier suppliers are based and how reliant the business is on them.

According to David Warrick, executive vice president at supply chain risk tech vendor Overhaul, companies need to negotiate more flexible contract terms moving forward to allow for quick supplier changes when necessary. They should also leverage dual sourcing agreements so that they can switch between suppliers to focus on sourcing goods and services from lower tariff countries. As the Trump administration has made clear, companies must move quickly to add tariff risk to their risk registers and monitor regional trade agreements so they can respond as rapidly as some of these policies are changing. Some experts believe companies need to go even further and actively engage with policymakers and the Office of the United States Trade Representative to influence tariff policies and seek exemptions or reductions. They could also consider engaging with lobbying groups to attempt to influence trade policy or apply for tariff exclusions.

Monitoring changes in tariff policies may also allow businesses to engage in "tariff engineering." This is when companies modify product design, classification or assembly locations to take advantage of lower tariff categories or duty-free entry. To ensure they

Shutterstock / Lightspring

comply with the U.S. International Trade Commission's Harmonized Tariff Schedule, which determines the tariffs imposed on different types of goods, companies can work with customs brokers to ensure they classify their products accurately.

Similarly, making use of foreign trade zones (FTZs) and bonded warehouses can also be a smart move for some companies. An FTZ is a secured location in or near customs and border protection (CBP) ports where product can be stored, exhibited, assembled, manufactured or processed without any duties being applied. This allows for duty deferral if the goods are eventually withdrawn into the U.S. customs territory or potentially no duties at all if the goods are shipped to another country.

Bonded warehouses provide similar benefits by allowing businesses to store imported goods under bond, deferring duty payments for a maximum of five years until the goods are removed for consumption. If the products are exported, no duty is owed.

Other programs can vary in their level of complexity. For example, through duty drawback programs, businesses can claim refunds on fees, customs duties and taxes paid on imported goods that are later exported or incorporated into exported products from the United States or that are destroyed. As it involves imports and exports, this is a complex process, but it can offer real duty savings for certain types of transactions.

Similarly, the U.S. Goods Returned program may allow some companies to claw back expenses. For goods that were initially exported abroad and then returned to the United States, such as for servicing, warranty services or value-added activities, companies may be able to declare an entered value equal to the value added abroad. If this is a common importing practice for the business, companies should check to see if they are taking advantage of the opportunities the program affords to minimize tariffs, Noh advised.

Another way to handle temporary imports to secure duty savings is to use a legal tool called a temporary importation under bond (TIB), which facilitates duty-free import into the United States for eligible goods being re-exported. TIBs cover a specific range of products and are good for a period of one year, though they can be extended in certain circumstances. They must be accompanied by a bond equivalent to twice the duty otherwise attributed to the import, but they allow companies not to pay duties for up to three years.

Insurance and Risk Management Considerations

Insurance policies may also provide some protection from tariff impacts. For instance, political risk insurance and trade disruption coverage may protect against sudden tariff changes and supply chain shocks. Political risk insurance provides coverage for businesses from financial losses caused by adverse government actions, and certain policies may be broad enough to cover retaliatory acts from foreign governments, such as reciprocal tariffs.

Trade credit insurance protects businesses against non-payment by customers due to insolvency, default or political risks. In the context of tariffs, such insurance coverage helps mitigate risk by ensuring companies can still receive payments from financially strained buyers impacted

"Tariffs can be more than a setback. But when approached with the right attitude, they can serve as a driver for smarter sourcing, stronger supplier relationships and long-term growth."

by higher costs. This would therefore reduce cash-flow disruptions and enable more flexible payment terms in uncertain trade environments.

Additionally, supply chain insurance can protect businesses against disruptions caused by events such as supplier insolvency, transportation delays or geopolitical issues. In the context of tariffs, this kind of insurance product helps mitigate risk by covering financial losses from supply chain interruptions, allowing companies to maintain operations and secure alternative sourcing without significant financial strain.

Companies also need to step up their own risk identification and risk management strategies to help offset the negative impacts of tariffs. First, Warrick recommended that risk managers conduct an immediate risk assessment to understand their organization's exposure to tariffs across the entire supply chain and map their supply chain to identify vulnerabilities and alternative sourcing options. A big part of such an exercise will likely need to include determining which of the goods, materials and suppliers that are susceptible to tariffs will have the greatest impact on business operations and costs. Furthermore, risk managers will need to evaluate alternative sourcing options to identify domestic and international suppliers that are less affected by the new regime.

Warrick said companies should have a workable tariff strategy so that they can determine whether to absorb costs or pass them on and determine whether to change supplier sourcing. Risk managers may also need to upskill to understand hedging strategies, such as future contracts on commodities affected by tariffs, so that they can recommend suitable practices for leadership to consider.

Risk management must work with other key operational and assurance functions like legal, finance, procurement and operations to develop cohesive strategies to address tariff impacts. This collaboration ensures that all aspects of the business are aligned and responsive to trade policy changes, Noh said, adding that risk managers should oversee the implementation of measures such as supply chain diversification, contract renegotiations and compliance audits to mitigate any adverse effects. "By proactively addressing potential vulnerabilities, companies can enhance their resilience against trade disruptions," Noh said. Risk professionals should also monitor regulatory developments. "Staying informed about policy changes, such as executive orders and trade agreements, allows risk managers to anticipate and prepare for shifts in the trade landscape. Regular engagement with industry news and government publications is essential for timely responses," she said.

Risk professionals also need to ensure that management has better real-time information about tariff and supply chain risks so that they can make more informed and agile decisions for different scenarios. For example, software tools can help businesses "analyze consumer behavior and competitor pricing to make targeted, strategic pricing moves instead of imposing blanket price hikes," said Edward Peghin, managing lawyer at Pace Law Firm.

The threat of escalating tariffs is naturally a key concern for companies. Businesses can also treat the situation as an opportunity to improve governance and increase resilience as they address the financial risks that tariffs are likely to pose. Forward-thinking companies can use the exercise as an opportunity to explore how they can gain greater visibility into and take greater control over their supply chains, which may provide more long-term assurance.

"Tariffs can be more than a setback," Peghin said. "But when approached with the right attitude, they can serve as a driver for smarter sourcing, stronger supplier relationships and long-term growth. Businesses that embrace adaptability and strategic planning will not only overcome tariff changes but may even gain a competitive advantage." R

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

Shutterstock / AndryDj

The Characteristics of Effective Risk Le

by John Hintze

Companies face an ever-growing list of risks in a variety of areas, from technology and finance to climate and geopolitics. A recent McKinsey & Co. study identified six "habits" of highly successful chief risk officers (CROs) that help them address those risks, build greater corporate resilience, and ultimately strengthen their leadership role within the organization.

The study primarily considered the role of CROs at financial institutions who historically focused on financial risks but now also address nonfinancial risks to bolster the bottom line. As the scope of risk management has broadened to include risks across the company, the CRO's role and leadership responsibilities have been elevated, making good habits more important. "CROs that have a broader grasp of some of those key areas are probably playing a more strategic role in their organizations," said Stewart Goldman, co-head of risk and compliance at executive search and management consultant firm Korn Ferry.

Not only do today's CROs advise corporate leadership on risks they identify throughout the business, they have also become the face of the risk appetite approved by management and the board, disseminating it through the organization and generally promoting a culture of risk awareness.

Playing off Stephen R. Covey's book *The 7 Habits of Highly Effective People*, the following habits—perhaps better described as practices—can help CROs be more effective and can serve as a guide for all risk professionals to "level up" and take a more strategic approach to risk management within their organizations:

Explain your risk and resilience vision and champion a risk-aware culture. According to Joseph Agresta, an assistant professor at Rutgers Business School and previously a procurement

Adobe Stock / Celt Studio

aders

Risk leaders need to not only create a risk management vision—what McKinsey refers to as the "North Star" of a successful CRO—but they must also develop a way to continually evaluate whether the organization is following it.

leader at Johnson & Johnson, it is important for CROs to clearly explain and champion their vision of risk and resilience to help create a risk-aware culture.

"If a company wants a risk culture, everyone has to think like a risk officer, so the visibility of the CRO and leading by example becomes very important," Agresta said. "The CRO should be working with [department] leaders to identify which corporate muscles need to be developed to strengthen the business so that, in a dynamic and changing environment, the company can react more quickly. They set that example by driving the conversation."

Risk leaders need to not only create a risk management vision—what McKinsey refers to as the "North Star" of a successful CRO—but they must also develop a way to continually evaluate whether the organization is following it, said Sim Segal, founder and director of Columbia University's master's program in enterprise risk management (ERM) and president of ERM consulting firm SimErgy Consulting. Segal recommends a value-based ERM program that allows organizations to focus on 20 or 25 key risks and calculate the likelihood of achieving or missing their strategic plans based on those risks. "That is the most important number for the organization," he said. "Everyone's job promotion and bonuses are tied to achieving that plan."

Invest in and empower the next generation of risk leaders. Today's complex risk environment requires building a diverse team from different backgrounds and perspectives and shifting staff roles, both within the risk function and among other parts of the business. This can create opportunities for team members to share insights and reinforce the risk culture.

In addition, identifying top performers and finding opportunities for them to interact with the company's top executives helps empower them for future growth and career elevation. "You do not want to be defensive of your own position; if [junior risk partners] are successful, you will be successful," former Goldman Sachs CRO Craig Broderick said in an interview with McKinsey. "A CRO should not be insecure in that regard. For a successful organization and a successful person, there is more than enough credit to go around."

Shutterstock / Philip Steury Photography

Engage deeply with C-suite leaders and the board to accomplish business resilience and risk objectives. Engaging with leadership requires a common language and measurement system, enabling CROs and risk leaders to clearly describe the risks bubbling up through the company to senior management and the board. Whether those risks stem from proposed business ventures or other internal or external changes, applying a methodical standard provides apples-to-apples comparisons to measure the impact of different risks.

Leading CROs do more than simply inform the board and the CEO—they are vital members of the executive team and trusted advisors to the board. In fact, the CROs that McKinsey interviewed said they spend up to 56% of their time with the executive team and board.

To quantify risk and measure its impact and probability, a common language is critical, Agresta said. For example, Johnson & Johnson developed a shared language and measurement system, dubbed the "80% standard" because 80% of the system could be used across all the company's numerous and varied functions, leaving 20% for business-specific areas. The approach was applied across the company's consumer, medical and pharmaceutical business lines, enabling the company's risk officers to use the same tools to generate a consistent register of risk.

"Based on that common language and system, the head of risk understands the process used to measure the risk and articulate it, and can then present it to appropriate leadership that prioritizes it and makes decisions," he said.

Treat department supervisors as partners. A common language and measurement system is equally important in the other direction, when risk leaders gather input from the supervisors of the company's other business units and functions. CROs should establish working relationships and find common ground with these business unit-level leaders, meeting with them often to discuss what is happening in their areas.

That has not always been easy for risk management, given that its role as a risk mitigator has often led to a reputation as a constraint on business leaders who want to take on additional risks to increase profits. Segal suggested that a risk management methodology like value-based ERM actually provides upside benefits as well, recasting CROs as arbiters of both risks to avoid and which ones to take.

Segal noted the importance of consistently applying a common methodology, including analytical tools, terminology and definitions. Different areas in a company often develop different cultures, whether due to experience, geography or other factors, and they may be tempted to tweak a methodology's inputs without alerting risk management. "If risk does not detect those differences, then it may be trying to add up apples, oranges and bananas," he said.

A common methodology enables risk management to analyze proposed changes arising from the company's business areas to determine how they increase or decrease the organization's risk and value. If the risk of a proposed change decreases corporate value, then risk leaders can offer insight into how to address weaknesses and provide upside instead. Risk professionals and department supervisors become partners. "Supervisors trust risk and see that it is not trying to block everything they are trying to do," Segal said. "The risk department is trying to help them measure the risk and make better bets."

Integrate insights across the organization to anticipate future threats and strengthen resilience. Integrating insights is just as crucial as explaining and championing a risk-aware culture, according to Segal. "You are gathering information from the company's leaders, but you are also subtly training them not to have groupthink, but to define risk," he said.

Risk is fundamentally an analytical practice and companies still prioritize prospective risk leaders' analytical abilities when hiring, according to Carl Gargula, executive vice president at Risk Talent Associates. Integrating—and communicating—insights across the organization is critical. "CROs must communicate down to their teams, up to management, and across and within the organization," he said.

Monitor personal effectiveness and take steps to manage time. McKinsey says risk leaders must reflect on their own effectiveness and be deliberate about how they spend their time, set goals and prioritize. This includes identifying strategies to maintain work-life balance, both for their own long-term sustainability and to motivate their team. To drive continual performance improvement, it is also essential to seek out feedback from peers and colleagues, particularly since the role of a risk leader cuts across the entire company and involves a wide range of issues and stakeholder demands.

Agresta said that such reflection should not only encompass a practical "what happened and how do we fix it?" approach, but also an element of compassion, or what he called a "servant-leader" mentality. "Sometimes risk events are very scary—a hurricane, a pandemic," he said. "As a servant-leader, the CRO must empathize with all the people impacted by the risk event, whether it is financial, supply chain-related or something else." R

John Hintze is a New Jersey-based freelance writer.

WE WANT YOU

...to share your ERM expertise with your peers.
Help create a stronger, more vibrant community of strategic and enterprise risk management professionals by contributing to *Risk Management*.

RISK MANAGEMENT

Visit **RMmagazine.com/contribute** for details on publishing your insights in *Risk Management*, the premier magazine for risk professionals.