RMmagazine.com

RISK MANAGEMENT

2024 ERM Special Edition

A publication of RIMS the risk management society

00

contents

COLUMNS

FEATURES

COVER: GETTY/ANDRII YALANSKYI; **THIS PAGE:** SHUTTERSTOCK/NADIINKO

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

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

www.RMmagazine.com

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 Mission Statement
When establishing a robust and meaningful ERM program, a vital first step is developing and memorializing a mission statement that explains its primary purpose. 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 "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 authoritative manual "sells" and guides your ERM program.

There are three 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

SHUTTERSTOCK/ANTON VIERIETIN

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 its 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, with the latter reflecting a 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 consistently and transparently, 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 is digestible.

For instance, you might 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 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 are vital to ERM success. Mere spreadsheets will not be sufficient. 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, and 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 fostering risk governance and risk culture. Keep in mind that simple descriptive identifiers (e.g., high, 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 several 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 any risk event whatsoever. 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 identifying and managing material risks. Policies are high-level approaches to decision-making, include significant discretion, and are often delineated in qualitative terms rather than strictly with 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 these tolerances are exceeded.

8. Actively Promote the Embedded Risk Governance Structure

ERM should never be considered a separate service function. Rather, look at it as a discipline consciously embedded in crit-

ical 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 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 potential loss. Establishing and enforcing 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 serve as an early-warning system to help companies effectively monitor, manage and mitigate risks.

10. Connect ERM with Other Risk-Related Disciplines

Once you construct and adhere to a robust risk management framework, risk-related issues can 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.

Do You Need a Risk Appetite Statement?

by Dr. Lianne C. Appelt

Most risk professionals are likely familiar with the concept of risk appetite and risk appetite statements. For the uninitiated, "risk appetite" refers to the level of risk that an organization is prepared to accept in pursuit of its objectives, before action is deemed necessary to reduce the risk.

In most organizations, risk appetite is implicitly or explicitly determined by the board of directors and/or executive leadership. The idea is that, by defining the amount of risk the company is open to, it can avoid the two extremes of uncontrolled innovation or paralyzing caution. This can be a helpful approach to risk management because it establishes set boundaries that the company can safely operate within and provides indicators of when risks fall outside of those thresholds. However, there is no "one size fits all" approach that works for every company, and not all companies are inclined to use risk appetite statements.

There are scenarios in which a company may not be keen to adopt the risk appetite approach, including (but not limited to) the following:

1. The company is not willing to make formal statements about risk appetite for legal or liability concerns. For instance, how would it look to investors if the board published a risk appetite statement that indicated an openness to taking on a greater level of risk in a certain area, and the company experienced a detrimental risk event? At best, it would look like the leadership was inviting this event, and at worst, the implications could put the company in jeopardy.

2. The company has had a risk appetite statement in the past and did not find it valuable. This could be because the statement was too broad, the objectives and strategies of the company did not align with the appetite statement, or communication around the risk appetite was insufficient.
3. The board and/or leadership team cannot agree on risk appetite in general. Misalignment and miscommunication around risk appetite can make it difficult to settle on an official statement.

Given the possible exceptions, the question is: Are risk appetite statements necessary? For purely regulatory reasons, especially in the financial sector, the answer for many companies is yes. However, deriving value from what can become a check-the-box activity is another story.

So, how can a risk practitioner maneuver in a situation in which there either is no statement at all or there is a perfunctory statement that does not tie to any actual risk management activities?

In the no statement scenario, without the boundaries or guardrails set by the board and senior leadership, it can be a challenge to know how much risk in each area of the business the company is willing to absorb in pursuit of its mission.

One way to overcome this is to assign responsibility to the lines of business. There is a substantial benefit to having the subject-matter experts in each area define the targets and/or thresholds around risk-taking. Not only do they have specialized

SHUTTERSTOCK/NICOELNINO

knowledge in the area, but they also have responsibility and accountability in ensuring that the business objectives are met. This vested interest makes developing a risk appetite determination especially meaningful as it will inherently be tied to actions, deliverables, key decisions and execution of tasks.

If it is not feasible to assign responsibility to the business for establishing risk appetite targets, an alternative approach would be to calibrate around the following questions:

- What decisions do we need to make to be successful?
- What can happen to prevent us from being successful?
- What information do we need to provide to our decision-makers?
- Who are our key stakeholders?
- Do we have agreement on the prioritization of risks?
- How can we monitor performance to know when a shift in strategy is required?

Sometimes, just agreeing on these questions is enough to ensure that risks are managed effectively. A specific risk appetite statement may or may not be necessary. Customizing your approach to the maturity of your business and the risk culture of the company often requires a bit of creativity.

Next, consider the scenario in which there is an existing statement but it does not connect to the business in a meaningful way. An ideal risk appetite statement will be: 1) linked to the company's core objectives and overall strategy; 2) forward-looking; 3) embedded into key business processes; 4) communicated effectively; and 5) actionable and/or measurable. Without those elements, tying risk appetite to the business or strategic decisions would not be possible.

There are a couple of ways to remedy this. One approach would be to move forward as if there is no statement at all, as in the previous scenario (i.e., assign each line of business to defining their own risk targets). Another approach would be to work with leadership to modify the risk appetite statement to include more of the essential elements needed to provide a meaningful boundary from which to derive a risk framework or plan.

In any of these workarounds, the critical piece is finding a way to tie established targets, thresholds, bounds or other elements back to executive leadership or the board to ensure that they align with the overall company strategy and are acceptable at all levels. Otherwise, you are still missing the mark from an overall enterprise risk management perspective.

In a 2018 article, *StrategicRISK* Asia Pacific editor Lauren Gow encouraged companies to "tear up your risk appetite document now" and instead refocus value on regular reviews of board-level policies and making risk recommendations. Her argument was that the status quo around risk appetite statements does not enable integrated ways of working. Instead, it creates unnecessary silos and barriers to effective management.

"In the creation of a specific risk appetite document, risk managers are essentially handing the board further ammunition to shorten the leash of management," she wrote. "You are adding barriers to management from a board level and making it more difficult for management to take a calculated risk on new products or markets. This goes against what most risk managers say they want to be seen as within their business."

Eliminating the risk appetite statement may be too bold a move for your organization, but risk management can operate successfully without one as long as core elements are established and agreed upon.

While risk appetite guidance, regulation and trends may change over time, one thing is certain: What works for one organization may not work for another. Risk professionals must use their knowledge, experience and judgment to determine the best approach to ensure that they are providing decision-makers with a path to appropriate risk-taking—with or without a risk appetite statement. R

Lianne C. Appelt, Sc.D., CISM, CISSP, RIMS-CRMP, is head of enterprise risk management at Salesforce. This article was adapted from the 2024 RIMS executive report *Developing and Refining Risk Appetite and Tolerance*.

New Emissions Disclosure Rules Create Challenges

by John Hintze

In March, the U.S. Securities and Exchange Commission (SEC) issued its final climate-related disclosures rule. The rule mandated that public companies disclose their climate risks and report on their greenhouse gas emissions. While implementation of the rule was temporarily paused in April amid various legal challenges, companies may still need to take action as other jurisdictions require such disclosures.

Indeed, companies face an ever-growing and more complicated web of emissions-related reporting requirements, including two California laws that were passed last October and are also currently on hold, and a rule in the European Union that requires emissions reporting starting next year. All three rule sets require companies to report on their direct greenhouse gas emissions (Scope 1) and the emissions associated with their purchase and use of electricity, steam, heat and cooling (Scope 2). The California and EU rules also require Scope 3 reporting of "value chain" emissions produced by a company's customers and supply chain participants worldwide. The SEC included Scope 3 reporting in its original proposal but omitted this requirement in the final rule.

California's law mandates Scope 1 and Scope 2 reporting in 2026 and Scope 3 reporting in 2027, while the SEC's requirements technically begin at the start of 2026.

The SEC's requirements are significant, but largely just codify what many companies are already doing. The requirements for registrants include disclosing the risks that have had or likely could have a material impact on their business strategies, operations or financial condition, as well as any measures to mitigate climate-related risks and the costs of those measures.

Registrants must also disclose any oversight of climate-related risks by their board of directors and management's role in assessing and managing those risks. In addition, they must disclose the capitalized costs, expenditures, charges and losses stemming from severe weather and natural events such as wildfires, and losses related to significant carbon offsets and renewable energy credits.

UNDERSTANDING THE STAKES

With key regulations on hold, companies may be tempted to delay compliance efforts. That may just be delaying the inevitable, however, and not just because the currently stated deadlines may still apply. According to Niamh McCarthy, director of climate-related risks at Orbitas Climate Advisers, many other countries, including Brazil, India and Japan, and states such as New York, Illinois and Washington, are pursuing or have adopted climate-related financial regulations. "Market leaders can see this surge in climate-related financial disclosures as an indicator of what is to come," she said.

Companies without physical operations in California or the EU that do not see the urgency in preparing for Scope 3 reporting may want to reconsider. For example, California's law will require public and private companies with at least $1 billion in revenue to comply with its GHG emissions-reporting requirements. Those with $500 million or more in revenue will be required to report climate-related risks and measures to reduce those risks both to the state and on company websites.

These requirements will apply if the

SHUTTERSTOCK/NADIINKO

company is doing business in California, which the state has interpreted in line with its tax laws to mean "engaging in any transaction for the purpose of financial gain within California," said Michael McDonough, partner at Pillsbury Law.

As a result, companies that have no physical presence in California may still be subject to the requirements. "If any part of their value chain happens there, the state could consider them covered," McDonough said. "Any company with $500 million or more in revenue is likely to have some financial interest tied to California transactions, such as customers buying its product and bringing it home."

TRACKING REPORTING REQUIREMENTS

A company's Scope 1 and Scope 2 emissions reporting requirements may not differ substantively between the SEC and California regulations as both require using the same international greenhouse gas accounting standards. The EU's Corporate Sustainability Reporting Directive (CSRD) sets out reporting requirements similar to those in the United States and includes Scope 3 reporting. The first wave of large EU companies subject to CSRD have to make disclosures in 2025, while large non-EU companies will begin in 2026 and smaller non-EU companies with EU revenue over €150 million will need to comply starting in 2029.

Even if Scope 1 and Scope 2 emissions disclosures to the SEC and California end up being similar, companies must still track regulatory developments, including when regulations are finalized and come into effect, and if there are any variances among them. There likely will be some administrative differences between the disclosure regimes, McDonough said, including the SEC's requirement to report "material" emissions, compared to California's requirement to report all Scope 1, 2 and 3 greenhouse gas emissions, whether the company deems them material or not. "Companies will probably start with the California data and may scale it back for the SEC," McDonough said.

U.S. companies with significant business in Europe may instead want to make their starting point the CSRD, since those regulations are final and include Scopes 1, 2 and 3 requirements. California's reporting requirements are also similar to the EU rules.

EVALUATING SCOPE 3 RISKS

Although the SEC omitted Scope 3 emissions reporting from its final regulation, companies still need to understand and evaluate how Scope 3 greenhouse gas emissions may represent material risks or opportunities to the business. Kristen Sullivan, an audit and assurance partner who leads sustainability and ESG services at Deloitte & Touche, said the SEC has emphasized the more traditional Supreme Court definition of materiality that includes the total mix of information available to guide investor disclosures. California's objective, on the other hand, is to promote transparency around climate-related risks.

As a result, companies providing Scope 3 emissions disclosures in compliance with California or EU rules will need to consider these broader disclosures when determining materiality for their SEC disclosures.

"The SEC is basically saying that if your company is making ESG disclosures elsewhere, this information should be considered when evaluating materiality—from a quantitative or qualitative perspective—for purposes of meeting investor expectations," Sullivan said. "Scope 3 emissions are not required by the SEC, but organizations will need a much more comprehensive analysis to determine what should or should not be included in an SEC filing."

For Scope 3 emissions, large companies will have to rely on the emissions calculations of often smaller and less resourced value-chain customers and suppliers. Therefore, CSRD regulations provide a three-year grace period in which financial statement preparers can omit Scope 3 emissions reporting and instead disclose why they omitted it and their efforts to obtain it.

McDonough said that the California emissions law requires companies to follow the reporting standards established by the GHG Protocol, including its guidance for using primary and secondary data sources such as industry-average and proxy data, and it may also allow additional information to inform Scope 3 estimates in the final regulations. He added that California's law essentially presumes that all greenhouse gas emissions are "material" and worthy of public disclosure, but the SEC regulations leave the determination of materiality to the company, and defining what is material in every situation may be challenging.

California's law mandates Scope 1 and Scope 2 reporting in 2026 and Scope 3 reporting in 2027, while the SEC's requirements begin at the start of 2026.

The more stringent standard will require companies to provide more detailed disclosures, increasing the risk of the SEC comparing the federal disclosures to those made to California and asking why a company did not include that information in its SEC financial statements. "California's requirements will probably end up dragging a lot of public companies to a higher standard of disclosures to the SEC, even if the SEC standards arguably do not require that level of detail," McDonough said. R

John Hintze is a New Jersey-based freelance writer.

Five Pressures Propelling Risk Transformation

by Tim Phelps

The evolving landscape in economic, geopolitical, regulatory and technological spheres has put a significant spotlight on the enterprise risk function within organizations. The role of the risk function is transforming from primarily mitigating threats to also identifying opportunities and contributing to the strategic direction of the company. Responsibilities are expanding beyond mere compliance to actively shaping strategies that enhance performance and fortify the competitive edge. Amid constant volatility, the risk function plays a pivotal role in ensuring organizational resilience and fostering trust among stakeholders.

The *2023 KPMG Chief Risk Officer Survey* captured the views of 390 U.S. enterprise risk executives and their perspectives about the next five years. Are risk functions ready to meet the demands of the future? What challenges are keeping risk leaders up at night, and what priorities are dominating their attention? How are risk teams evolving to optimize how they proactively support organizational objectives and meet regulatory expectations?

The survey data provides insights on how the following five mounting pressures are accelerating changes in organizations' risk management strategies, structures, processes and capabilities—and the challenges and opportunities to come on the risk transformation journey.

SHUTTERSTOCK/PIXEPIXELBLISS

DE-RISKING

Macroeconomic uncertainty is straining risk leaders' ability to keep pace with change. The survey identified regulatory and compliance risks, economic downturns and geopolitical volatility to be among the top future risk challenges, all of which many executives feel insufficiently prepared to tackle. These challenges are exacerbated by "compound volatility" due to cataclysmic disruptions—such as climate events, major bank failures, wars and supply chain failures—occurring at greater frequencies and intensifying the overall level of risk.

Although 80% of risk leaders reported being well-equipped to address cybersecurity risks, barely one-third of companies use predictive modeling and automation to anticipate potential risks. To proactively tackle emerging risks, organizations must invest in a centralized risk technology architecture, advanced data analytical capabilities and technology integration to enable the risk function to execute its high-stakes activities with greater speed, precision and agility. Allocating more resources to understanding and planning for "tail risks" can better hedge against the impact of unusual risks.

GROWTH OR STRATEGIC CHANGE

From new technology to shifting markets and customers, the rapid pace of change across the business landscape presents opportunities for agile, forward-looking companies to improve performance. But to take advantage, organizations must manage new and changing risks in a way that supports the business strategy. Strengthening risk strategy alignment with the business objectives ranked as one of the top three goals for risk professionals.

In terms of sufficient budget, attention to risk management and overall alignment with business strategy, 82% of respondents

reported receiving a high level of support from the C-suite. To make progress toward strategic enterprise risk management, incorporating shifting risks and strategic changes into the risk framework should be a key risk transformation goal, including providing training and resources for employees on risk management and corporate strategy alignment; analyzing risk mitigation successes and updating the corporate strategy; and fostering a strong risk and compliance culture as an enterprise-wide strategy.

REGULATORY COMPLIANCE

Regulatory compliance is the top risk management challenge for organizations over the next two to five years. With global regulatory authorities actively using regulatory change as a policy execution tool, there is increased pressure from government agencies to integrate new requirements and be compliant. In fact, CROs say regulators are putting the most pressure on the risk management function.

The evolving regulatory environment demands a more proactive and agile risk management culture—one that is primarily driven by strategic inputs, rather than operating in response to regulatory demands. to improving overall performance and supporting smart business growth it is critical to move beyond a compliance-centered approach focused on satisfying requirements and incorporating risk considerations into broader business strategies.

EFFECTIVENESS AND EFFICIENCY

Today's risk functions face a tall order: to actively contribute to their organizations' long-term viability, growth and trust. Eighty-eight percent of companies are set to increase their risk management budgets by at least 5% within the next 12 months, with AI and machine learning emerging as key tools for accelerating risk control processes.

Capitalizing on technology convergence will be key to driving specific business outcomes and enabling the risk management ecosystem to adapt and improve over time. The top measure for empowering risk teams was improving data and analytics capabilities, followed by increasing training for employees in targeted areas, and increasing diligence in policy management and employee accountability. Risk executives must align digital acceleration with the organization's transformation goals, including fostering an integrated, digital-first strategy and operating model, as well as acquiring or upskilling talent to meet new challenges, particularly in technical risk areas.

COST TAKEOUT

The cost to maintain effective risk management programs is at an all-time high. While labor typically constitutes the largest portion of risk operating costs, outsourcing offers potential efficiencies and cost reduction benefits. However, firms must always remember that they are outsourcing the risk management activity, not the risk itself. About one-third of companies are considering outsourcing across various risk management areas, such as strategic risk planning, financial risk analysis, cybersecurity and technology-driven threat protection.

It is crucial to carefully weigh the benefits of outsourcing against the need for adequate risk control, governance and sustainable savings. Risk leaders should develop and implement a strategic operating model that balances costs and effectiveness, leveraging technology, location strategies and global talent pools. Cost-saving strategies may differ across organizations but may include entity rationalization, product and channel simplification, operational model centralization and consolidation and automation of risk management processes.

THE WAY FORWARD

The strategic scope for the risk function now includes driving cost efficiencies, ensuring compliance and delivering business growth. It goes well beyond what has been traditionally expected from the function. To enable the risk function to deliver, leaders will need to be comfortable with uncertainty and double down on value drivers to navigate threats earlier and more effectively.

As new risks emerge, understanding the interplay between them will be crucial to define long-term mitigation strategies and resource allocation. While technology is playing a key role in enabling this transformation, culture and people are also critical success factors. Ultimately, organizations that look beyond compliance and cost-optimization, and integrate risk management as a strategic component of their value chain of the business, will come out on top. R

Tim Phelps is a risk service leader at KPMG LLP.

SHUTTERSTOCK/MALCHEV

IS YOUR BUSINESS FUTURE-PROOF?

by Neil Hodge

For many companies, it is hard to imagine no longer existing in a decade's time, but a growing number of chief executives believe such a scenario is frighteningly plausible. According to PwC's recent *26th Annual Global CEO Survey*, nearly 40% of CEOs do not think their company will be economically viable 10 years from now if it continues on its current path. Key factors cited included changing customer preferences, regulatory change, skills shortages and technology disruption, as well as the transition to new energy sources, supply chain disruption and the threat from new entrants. Nearly three-quarters of CEOs in Japan and 67% of CEOs in China did not believe their current business model would be viable in 10 years, while at the other end of the spectrum, only 22% in the United Kingdom and 20% in the United States were similarly concerned.

These viability concerns underscore the need for companies to reinvent themselves and reimagine what is possible, rather than stick with the status quo, PwC said. For example, Netherlands-based lighting turned audio/visual business Philips refashioned itself as a health technology company by bringing together the multinational's consumer-insights capabilities, expertise in medical-device technologies, and strengths

in data analytics and artificial intelligence. The company also exited some businesses, including its original lighting business, and de-emphasized others. As Frans van Houten, Philips CEO from 2010 and 2022, told PwC, "I recognized that the chances that we would transform lighting and health care simultaneously were not so high. And so we made a choice."

As companies work out their value proposition and future customer base, similar transformations are likely. "Chief executives now perceive more risks to the business than ever before and see their companies as being more susceptible to changing dynamics that can shift quickly and fundamentally," said Andrew McDowell, partner at Strategy&, PwC's consulting business. "As a result, what a company's core business might be today may not be its core business in just a few years' time."

Immediate, Intermediate and Long-Term Actions

Many share McDowell's view that companies may be forced to substantially transform if they are to stay in business. Andrew Hersh, CEO at risk services firm Sigma7, said the threat of some businesses failing within 10 years is "very real," fueled by key drivers like the rise of industry disrupters; macro-economic factors, such as inflation and supply chain problems caused by geopolitical risks; and the negative impact of regulatory policy and government intervention.

Hersh believes there are immediate, intermediate and future threats companies need to prepare for and which "should act as a galvanizing principle to take action now." In the immediate term, companies should use the resources and skills they already have to determine where risks and opportunities lie. "Companies need to look at how they operate and work out what changes can be made quickly and easily to reduce costs, free up resources and create improvements," he said. "The key is to use existing resources more efficiently and effectively to help make smarter decisions over the longer-term."

In the intermediate term, companies need to consider what changes are likely to occur in the next couple of years, assess the impact these might have on the business, and prepare the business to react and reposition itself as necessary. In particular, companies should have two key intermediate-term trends on their radar: energy supply and pricing, and customer behavior. "The invasion of Ukraine has demonstrated how susceptible European companies, in particular, are to dips in energy supply and hikes in energy costs, as well as the disruption both can have on their supply chains and production cycles," Hersh said. "Meanwhile, companies need to remember how the pandemic has shown how quickly customers can switch their priorities to suit their own needs."

Companies will also need to consider the long-term viability of how the business currently operates. "Will the organization need as many physical sites to operate from? Will AI and emerging technologies change product design and service delivery? Will companies continue to source key components such as electronics and microchips from China and other low-cost countries? It is obvious there is going to be a much greater need for better scenario-planning going forward," he said.

To cope with such change, companies need to implement a long-term strategy and review it regularly, ideally quarterly. "They should also consider what could kneecap it from succeeding," Hersh said. This includes reviewing whether the business has the right amount of capital to adjust to potentially seismic changes in the marketplace and whether it has the right machinery, IT capability and people to change direction quickly.

The Importance of Flexibility

For many businesses, survival may hinge on the ability to pivot when situations require it. However, the way many companies prepare for such contingencies often means there is a ready-made, prescriptive action plan in place for them to follow, rather than a built-in capability to react to the unknown.

"There is a tendency in many organizations, especially larger ones, to encode a system of policies that are designed to maintain stability and oversight," said Dr. Elizabeth Moore, head of leadership at the U.K.'s University of Law Business School. "Unfortunately, what often happens is that the organization gets strangled by its own rules and systems, which are no longer fit for purpose. Businesses need to maintain stability through uncertainty. To do this, they must be willing to create flexible internal systems that allow for change rather than rigidity."

To leverage opportunities from risk, organizations "must look at where gaps have occurred in moments of upheaval and consider strategies for taking advantage of those gaps," Moore said. However, it is challenging to maintain a balance between staying the course and responding effectively to a new situation.

"Companies that fare best in these situations will be those that have a flexible and resilient infrastructure; those that have made contingency plans for worst-case scenarios; and those that have built positive and transparent relationships throughout the various levels of management," Moore said. "When the crisis comes—and it will—the willingness of diverse individuals throughout the organization to work together to come up with solutions and find new opportunities

will be the essential foundation leading to the organization's success."

Some industries—namely the financial services and technology sectors—may be better prepared for disruption and substantial change than others, partially because these industry executives are "acutely aware" of the limited timespan and appeal of their offerings. Such awareness "prompts them to think their organizations are only six months away from bankruptcy," said Damian Handzy, managing director for risk technology vendor Confluence's analytics business.

"There is no financial services firm alive that thinks it has a 10-year lifespan continuing as it does now," Handzy said. "The sector is so competitive and prone to new disrupters that many firms think they need to overhaul their strategies and change within three years if they want to stay in business."

The financial services industry may also be better prepared for disruption because it has consistently sought to attract talented individuals that thrive on challenge to work on managing risks in key service areas and rewards them with generous remuneration packages.

"Since the 1990s, the financial services industry has sought out the best people from academia and other industries who are good with numbers and analyzing data to help assess not just organizational risks, but risks associated with new products, complex instruments and emerging trends," he said. "And

"Chief executives now perceive more risks to the business than ever before and see their companies as being more susceptible to changing dynamics that can shift quickly and fundamentally."

To leverage opportunities from risk, organizations "must look at where gaps have occurred in moments of upheaval and consider strategies for taking advantage of those gaps."

it has paid them far more than they would ever get anywhere else. While these institutions are not immune to failure, the industry as a whole is good at recognizing what needs to be done to survive and is also good at taking the necessary steps to avoid becoming obsolete."

Improving Decision-Making Through Better Risk Intelligence

Many experts believe better data collection and interpretation will be vital in enabling the kind of decision-making that underpins any business transformation, regardless of industry sector. Since the financial crash of 2008, companies across a variety of sectors have focused on putting controls in place to mitigate risks as they occur. However, they have largely done this in a patchwork fashion rather than as part of a coordinated, holistic effort to improve the risk management framework.

As a result, Rupal Patel, head of insights and risk intelligence at IT vendor Acin, said companies "have created their own operational risk" because they have likely duplicated controls to such an extent that the flow of risk and operational data is being slowed down, which is impacting decision-making.

"There needs to be an end-to-end view of data to understand the risks to the business and the opportunities that could be leveraged," she said. "Risk managers need to push for a better culture of 'tone from the top' to involve executives more in ensuring that data quality is maintained and that data is easily accessible and up to date."

Companies are also putting themselves at risk by failing to understand the importance and potential impact of non-financial risks to the business and not treating them as equally important as financial risks.

"Non-financial risk gets relatively little discussion in the boardroom as compared to financial risk, even though one impacts the other," said Damian Hoskins, operational and climate risk specialist at Acin. "Executives are much more comfortable discussing market and credit risks than they are non-financial risks because they have been told to look at the numbers all their lives. Risk managers will need to continue to push for a broader discussion of both sets of risks so that executives can decide future business strategy more appropriately and effectively."

According to Edgar Randall, managing director at business intelligence firm Dun & Bradstreet, companies need to have access to real-time information to facilitate more effective management decision-making. However, many companies are already disadvantaged compared to new entrants. "Disrupter firms, which are usually smaller, better resourced with the latest technology, and focused on a few core areas, are able to do this very easily and have leveraged data very aggressively to gain market share," he said. "More traditional players, on the other hand, tend to suffer because they have legacy IT systems that prevent them from innovating and using data more smartly. These companies have tons of data but they cannot do anything with it."

Risk professionals should improve the decision-making process so management can focus on core business risks. "If you look at the financial services sector, high volumes of automated decisions are carried out each day," Randall said. "Companies in other industries need to follow suit. Risk managers should push for more automated decision-making for 'low-risk' tasks so that management time is concentrated on getting better

SHUTTERSTOCK/IR STONE

information to inform more strategic issues."

According to Dr. Clare Walsh, director of education at the Institute of Analytics, data analytics is "crucial" to ensure a better understanding of risks and opportunities for any business. However, effective analysis is dependent on the quality of the data, using the right analytical tools and taking the appropriate action.

"Using flawed, incomplete and inaccurate data is obviously going to skew any results, while a reliance on basic and error-prone tools such as Excel is going to produce poor results and lead to bad decision-making," she said. "But even if data quality is good and the right tools are used, if executives don't act on the information they have, the whole exercise becomes pointless. It can still be a challenge for chief data officers and risk managers to convince CEOs about what the data actually means and what insights can be drawn from it to inform strategy."

Risk managers need to do more to show executives that data analytics can help inform future strategy and make business operations more resilient. This can be achieved by using clear metrics to show how much better off the organization is as a result of using improved data flows and more informed analysis. Risk managers "should pursue quick and easy wins that will show results in two months rather than two years," Walsh said.

For example, data analytics may show a retailer that poor complaint handling is contributing to declining customer retention rates. Consequently, they could implement a system that prioritizes emails and social media posts criticizing the company and sends them to the customer services team so they can tackle complaints more quickly. Data analysts and risk managers can then demonstrate the increase in sales, customer retention rates and speed at which complaints are addressed, as well as any decrease in refunds and number of complaints made, and show the impact on the company's financials.

Overall, McDowell believes one of the key contributions risk managers can make is to perform more of the "day to day" risk operations and prioritize risk reporting more appropriately so that executives can focus on long-term strategy. "For the past couple of years, boards have been busy stamping out fires rather than thinking long-term," he said. "As a result, risk managers will need to be more proactive in future. They will need to take greater control over how smaller, transient risks—such as some regulatory or inflation-related risks—are managed so that CEOs are free to focus on strategy."

Accounting for Talent and Staffing Risks

Technology is obviously important, but if companies want to survive, they also need take people into account. "Employees drive change as much as technology," said Dr. Alexandra Dobra-Kiel, innovation and strategy director at behavioral sciences consultancy Behave. If companies are going to adapt, they need to convince staff at all levels that the process is necessary, beneficial and achievable, and be transparent about how they intend to proceed. "You need to have a scenario in mind that sets out what the plans are for the future and the steps you will take to get there," she said. "You also need to be clear that there will be risks, but that the benefits will outweigh these."

Companies also need to make judgment calls about whether their current staff and leadership team have the skills and expertise to make the changes. "Not everyone in the organization will be capable of meeting the expectations that change demands, while others might be frightened by it, so recruitment and retention strategies become very important," Dobra-Kiel said.

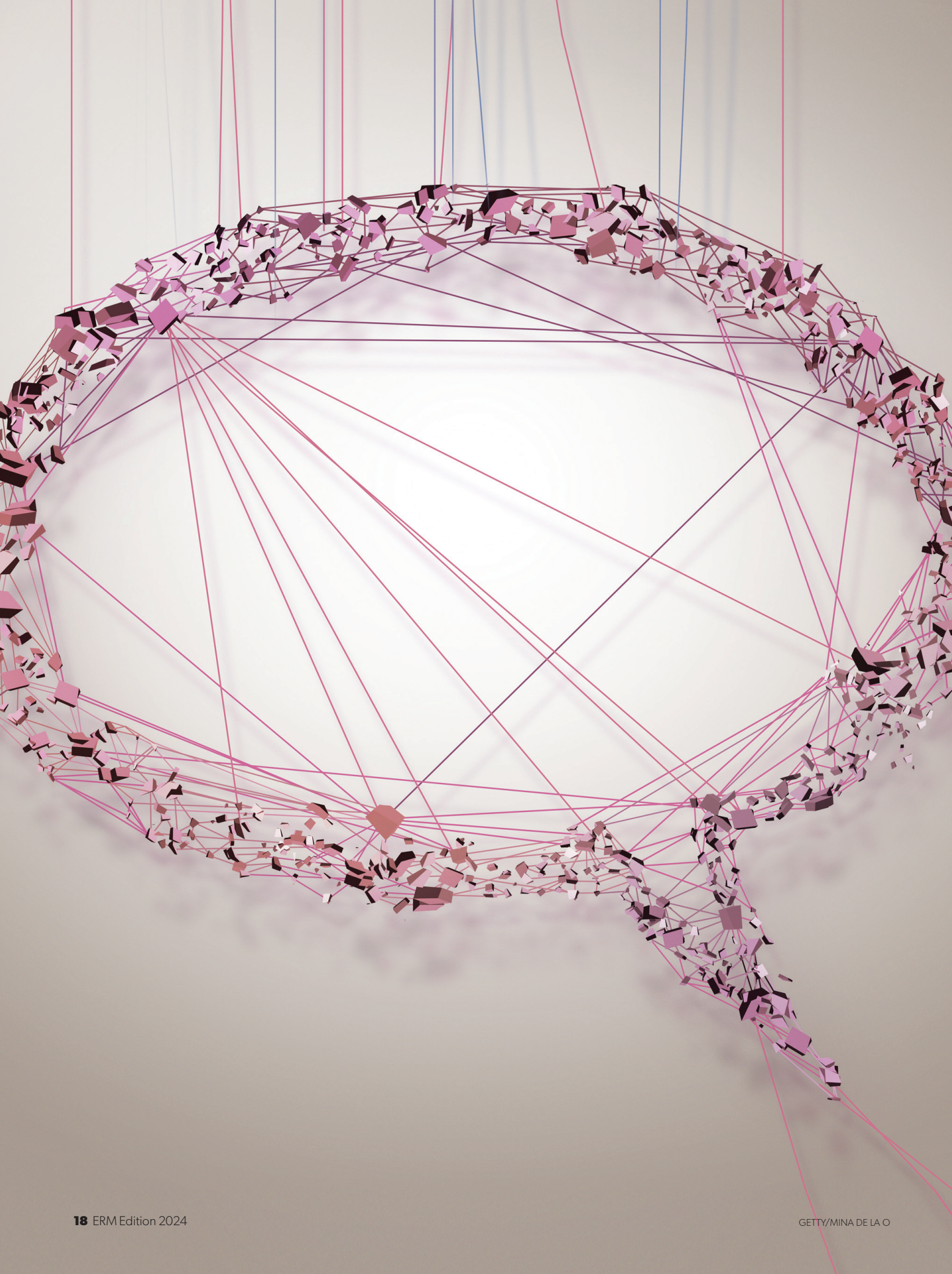
However, she cautioned against only hiring people with "gung-ho" attitudes who seem to relish difficult challenges. "Change is not reckless—it has to be well-planned and well delivered," she said. While many companies assume it may be as simple as hiring eager young workers to execute dramatic changes, this is not an advisable strategy on its own. "Bringing in new blood of typically younger people who are ambitious, confident, aggressive and seeking challenges may not necessarily be the best answer in all scenarios," she said. "Also, these people are unlikely to understand the company's culture, so they may clash with existing key staff that the organization also needs."

Improving Stakeholder Relationships

The global economic and geopolitical upheaval of the past few years has demonstrated how long-established business models can be shaken to their core and how quickly customer behavior can change, forcing companies to adapt accordingly.

Moving forward, companies' survival will depend on having a better and deeper relationship with a wider range of stakeholders. "CEOs need to know what their stakeholders expect from the company over the long-term and how it will achieve its strategy and goals," McDowell said. "Companies will need to explain their value proposition carefully to engender trust, taking into account issues such as climate risk, sustainability and ethics. Companies risk alienating key groups of stakeholders who will simply look elsewhere to do business if they don't listen to or ignore their concerns." R

Neil Hodge is a U.K.-based journalist who frequently covers risk management topics.



GETTY/MINA DE LA O

Strategic Storytelling:

How to Amplify Your Impact and Drive Better Risk Management Discussions

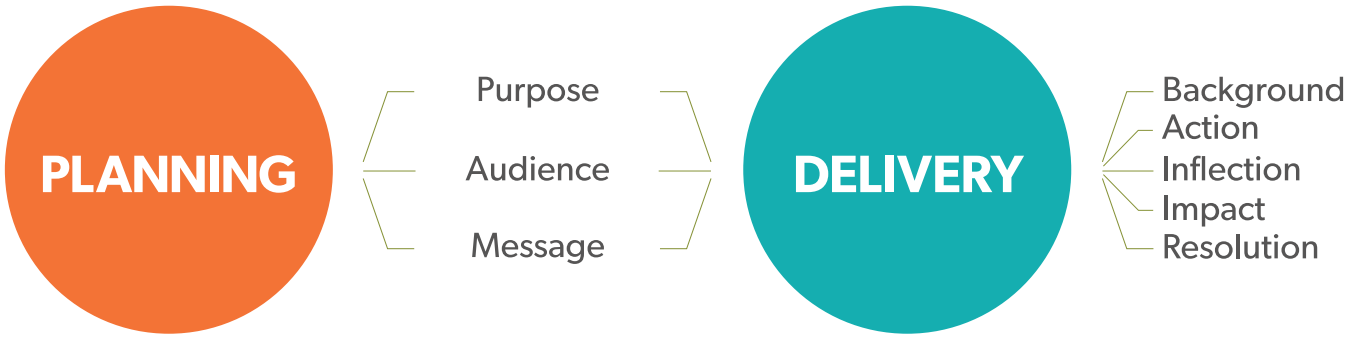
by John P. Angkaw

Over the past several years, organizations have faced unprecedented challenges and uncertainties. In response, many were able to adapt to their new risk environment by revisiting the way they do business and placing a greater emphasis on stability and long-term sustainability. This approach elevated risk management as a key enabler for achieving the organization's goals as enterprises increasingly adopted risk management practices to inform short- and long-term strategies, establish effective engagement with stakeholders, and conduct rigorous scenario-planning.

In the process, the role of the risk professional is beginning to move from that of a risk advisor to more of a trusted strategic business partner. As part of this shift, risk professionals will need to expand their skillset to synthesize complex information and convey it in a manner that is understandable and relevant to a diverse set of stakeholder groups, ranging from boards of directors to frontline staff.

Many risk professionals have benefited from adopting strategic storytelling as a useful communication technique to better engage stakeholders and advance the organization's risk culture. The following outlines a strategic storytelling framework that can be tailored to meet the unique needs of any risk professional. To help illustrate its applicability, two scenarios commonly encountered by risk professionals will also be discussed in the context of each step of the framework.

Strategic Storytelling Framework



PLANNING

The strategic storytelling process begins before you ever engage with stakeholders. During the planning phase of the communication, it is important to identify the purpose, the target audience and the message you intend to convey.

Purpose: Incorporating strategic storytelling as part of a communication plan requires prior reflection on the intended purpose and outcome of the message. Consider the reason for delivering the intended information to the target audience and how storytelling can amplify its reach and impact. Then, determine whether the message is intended to inform or drive action, which communication channels to utilize, and what platforms you will deliver it to. Identifying the intended purpose of storytelling will inform the subsequent techniques that will be required to achieve the intended objective.

Scenario 1: Sharing Information

Purpose: For information
Channel: In-person and email
Platforms: Executive leadership meetings, division leadership meetings

Scenario 2: Obtaining Approval

Purpose: Gain approval/agreement
Channel: In-person
Platforms: Board of directors meetings, executive leadership meetings

Audience: Identifying the target audience is critical to ensure that the key messages reach the appropriate groups and individuals. You will need to identify and analyze the various groups and individuals impacted by the information. These groups can be internal, such as the organization's board of directors, leadership or staff, or external, such as vendors or community partners. As part of this process, categorize the stakeholder types (e.g., primary, secondary, tertiary) as this will help define each group's degree of vested interest and the relationships among these groups and individuals. It will also help inform decisions about the appropriate communication channels to use.

Scenario 1: Sharing Information

Target Audience:
- Executive leadership
- Division leadership
- Division stakeholders

Scenario 2: Obtaining Approval

Target Audience:
- Board of directors
- Executive leadership

Message: Determining the key messages or objectives of the communication plan will help you ensure that you deliver the main points of information to the target audience. Messages should comprise the information, ideas and positions that support achieving the overall goal. Understand and address the unique perspectives, preferences and needs of the various stakeholder groups and tailor the messages accordingly to achieve the intended purpose for each target audience.

Scenario 1: Sharing Information

Key Messages
- To share an update related to the annual risk assessment
- To outline the process involved in the risk assessment
- To reflect on previous challenges in identifying risks
- To highlight actions taken to improve the risk assessment
- To articulate the results and focus moving forward

Scenario 2: Obtaining Approval

Key Messages
- To obtain approval for the annual risk management plan
- To outline the process involved in the risk assessment
- To reflect on previous challenges with risk management program
- To outline actions to recalibrate the risk management program
- To highlight the risk management plan and focus moving forward

DELIVERY

Once you have completed the planning process and understand your purpose, audience and message, you can craft your story to deliver information in a way that more effectively engages stakeholders.

Background. To start, establish the context or backdrop of

RIMS Risk Maturity Model®

WHAT

The **RIMS Risk Maturity Model®** (RIMS RMM®) is a self-assessment designed to help you identify the strengths and weaknesses of your organization's risk strategy. The RIMS RMM® was built for risk professionals, by risk professionals.

The model focuses on the elements ("pillars") and characteristics ("attributes") considered most important for maturing risk management capabilities.

RIMS RISK MATURITY MODEL® Pillars

STRATEGY ALIGNMENT
Degree that decisions integrate risk, results, and threats to the strategy itself.

CULTURE AND ACCOUNTABILITY
Degree that risk considerations are pervasive from the governing body to the front line personnel.

RISK MANTAGEMENT CAPABLITIES
Degree of organizational and individual learning and development with respect to managing risk.

RISK GOVERNANCE
Degree that the enterprise risk management discipline influences and interacts within an organizational risk ecosystem.

ANALYTICS
Degree to which an organization uses technology and analytics to establish, collaborate, gain insight and maintain connections with stakeholders.

This Risk Maturity Model helps you establish a baseline of risk maturity. Once you know that, you can determine the risk maturity level most beneficial to your organization for managing change and getting your organization future ready. Your RMM report measures your organization against five pillars and 35 attributes that leading risk management professionals believe are most important for success. How does your organization compare? Find out at www.RIMS.org/RMM.

PRICING	RIMS Member: Included in membership	Non-member: US $199 the first year, US $99 after

To take the RIMS RMM® assessment, visit www.RIMS.org/RMM

RIMS® the risk management society

the story. This requires providing information about "what," "when," "where," and "who." You will need to identify the scenario/issue, provide the context surrounding it, outline the main characters or stakeholders, and explain the degree to which they are impacted. Then, you can address the "why" by articulating the relevance of the scenario/issue and the circumstances arising from it.

Scenario 1: Sharing Information

"During the time we have together, I will be sharing an update on the annual risk assessment, which will serve as a key component of the annual risk management plan and the important work that all of you do as executive and division leaders.

"As you may recall, the risk assessment was conducted earlier this quarter and involved an extensive process conducted by the risk management team with each of the divisions. As part of this process, we have had detailed discussions with each of the divisions to review their respective risks and assess their likelihood, impact and velocity using a standardized taxonomy and rating scale."

Scenario 2: Obtaining Approval

"The purpose of this meeting is to present the annual risk management plan for the business and seek this group's approval.

"As many of you are aware, the organization establishes an annual plan to guide risk activities across the organization and serves as a key enabler for achieving the organization's strategic mandate. As part of the process to establish the annual plan, we have worked extensively with each of the divisions across the organization to review their risk profile and establish risk management controls and strategies in alignment with their risk appetite."

Action. Once the background has been conveyed, outline the events that have taken place and how they affected the main stakeholders involved. This can include reviewing the challenges and conflicts that led up to an inflection point requiring a significant action or decision to be made by the stakeholders. This progression of events makes the case for the stakeholders to take action or make a decision that balances varying perspectives and values, including their own.

Scenario 1: Sharing Information

"Leading up to this point, you will recall that the organization was challenged as it had a decentralized approach to identifying risk throughout the organization. As a result, there was no coordinated approach to engaging stakeholders across the organization and no standardized approach to capture holistic feedback in relation to the risks facing the organization. This often led to confusion and lack of clarity for the risk assessment and the entire risk management program as a whole, which contributed to the lack of buy-in to the risk management program."

Scenario 2: Obtaining Approval

"Over the past several years, you will recall that the organization had a risk management plan in place. While the previous plan had its strengths, it also had flaws as it did not provide the depth and breadth in its approach appropriate to the size and complexity of the organization. As a result, there were often challenges with identifying and addressing risks in the appropriate manner, which led to the uncoordinated deployment of resources to manage risks across the organization, leading to further exposures."

Inflection. Once the challenges, conflicts and progression of events have been articulated, you should outline the actions or decisions that have been taken. This is a pivotal moment in the story where key steps and measures are taken in response to the events. Specifically, this can include highlighting the opportunities that were available and steps taken to evaluate the different courses of actions and decisions in pursuit of the desired outcome. It is at this point that the core values of the story (or of the organization itself) are put to the test and placed into action.

Scenario 1: Sharing Information

"In response to the challenges associated with the previous approach, we conducted a review of the risk management program, including the risk assessment approach. As part of this, we conducted a review of best practices and benchmarking with peer organizations. We also consulted with each of the business divisions across the organization to obtain feedback on opportunities for improvement."

Scenario 2: Obtaining Approval

"To address the challenges that we experienced with the previous plan, we initiated a comprehensive review of the risk management program, including key services and deliverables such as the annual risk management plan. Through this work, we consulted with external and internal stakeholders to obtain insight and feedback on how we can advance the risk management program."

Impact. After conveying the inflection point, the next step is to outline the aftermath, including the direct and indirect impacts to the respective stakeholders. Specifically, you can provide details on the varying perspectives held by the stakeholders toward the actions or decisions that have been taken and the resulting consequences. Additionally, this can include articulating the eventual return to normal or introduction of new challenges or conflicts, which may require further action from the characters/stakeholders in your story.

Scenario 1: Sharing Information

"The review provided valuable lessons and insights that served as important input as we looked to improve the risk management program, including the risk assessment process. The steps we took resulted in the establishment and provision of role-based risk management training for individuals and groups across all divisions, development of a standardized risk assessment form and a simple step-by-step process to complete the assessment within each division."

Scenario 2: Obtaining Approval

"The program review provided us with the opportunity to gain new insights on steps we can take to improve the program, services and deliverables. As part of this work, we have been able to strengthen the risk management program, including the adoption of an overall framework that provides guidance to risk management activities across the organization and divisions. In addition, we have taken steps to enhance and streamline our approach in how we identify, assess, monitor and evaluate risks."

GETTY/DRAFTER123

Resolution. The last part of the story should focus on summarizing results and addressing the current status. Articulate what has changed since taking decisive actions or making decisions in response to the particular scenario or issue. In addition, this step can be used as an opportunity to emphasize key messages, perspectives, actions or decisions made during the story, while sharing some of the lessons learned throughout the story.

Scenario 1: Sharing Information

"With your support, we have been able to make strides in improving the risk assessment approach in the organization. This has led to a more effective and efficient approach to identifying the organization's risks, and it has also allowed us to build a strong foundation for the risk management program that we can build upon moving forward."

Scenario 2: Obtaining Approval

"With the program review and the changes we have been able to make to strengthen the risk management program, we are well-positioned to support the organization to move forward and achieve its strategic mandate. We will be better able to manage risks and opportunities through more informed dialogue and decision-making across the organization."

PROVIDING STRATEGIC VALUE

As organizational goals evolve, some risk professionals are taking on a greater strategic role. By incorporating the strategic storytelling framework into their practice, risk professionals can amplify their reach and impact as strategic business partners, advance organizational risk initiatives, and drive meaningful dialogue and informed decision-making that will result in sustained value for their respective organizations. R

John P. Angkaw is vice president of the public entity group at Marsh Canada Limited.


CPU
62 %
CPU

The Impact of AI on Insurance Underwriting

by Neil Hodge

The increasing acceptance and adoption of artificial intelligence in the insurance industry promises to have a significant impact on insurers and insureds alike. The ability to analyze large datasets quickly and effectively will allow insurers to understand risk as never before, leading to more accurate risk identification, improved underwriting and claims handling, and better premium pricing.

The technology does not come without risks, however, as important questions remain around the accuracy, fairness and security of AI-driven processes and decision-making. Therefore, insurers and risk professionals need to better understand the potential pitfalls of AI technology and take steps to ensure that the process of purchasing insurance does not introduce greater risks than what it was intended to cover.

AI Bias in the Underwriting Process

AI can bring more precision to actuarial models and underwriting, allowing insurers to provide tailored coverage to their client base and bolster risk management. The technology can also improve risk assessment and underwriting by analyzing vast amounts of information from diverse data sources, including internal data such as historical claims and customer behavior, and external data such as litigation trends, market changes, extreme weather events and social media posts. This data enables insurers to establish a more comprehensive understanding of risk factors and thus allows

ADOBE STOCK/SUMMIT ART CREATIONS

for better and more specific underwriting decisions. Additionally, insurers can use AI algorithms to create more personalized insurance policies that are based on individual behavior, preference and risk profile, resulting in a more bespoke set of coverage options that should better satisfy customers' needs.

Despite the benefits, experts warn that the insurance industry is not immune to the same problems associated with AI that have impacted every other sector—namely, the risks of bias, data misuse and data insecurity. As a result, risk professionals need to ask for more details about how AI is used when underwriting their company's policies and what checks and balances are employed to ensure the accuracy of results.

According to Wilson Chan, CEO at AI fintech firm Permutable AI, it is "absolutely critical" to address the repercussions of biased data on AI systems within the insurance industry. "Companies often face inflated premiums and coverage restrictions due to insurers training their underwriting AI on limited or biased data," he said. "The inherent nature of AI systems means that if the input data is biased, the decisions made by the AI will inevitably reflect those biases. To ensure fair treatment in insurance purchases, companies must engage insurers with crucial questions about the training data, its bias mitigation, and the transparency of AI-driven decision-making."

Insurers must be certain that AI systems are trained on representative, unbiased data, and that they regularly review and update AI systems to eliminate biases. They also need to provide transparency about the functionality of the AI systems they are using and what processes AI is being used in. "By adhering to these measures, both companies and insurers can contribute to the fair and responsible use of AI systems in the insurance industry," he said. "This commitment to transparency, unbiased data and ongoing vigilance is fundamental to fostering a trustworthy and equitable insurance landscape."

To illustrate the risk of biased decision-making, Chan offered an example using flood risk insurance. "In this instance, AI models trained on historical data might unfairly impact companies in areas prone to increased flood risk, overlooking current climate patterns," he said. "This could result in companies facing higher premiums or coverage limitations, irrespective of the mitigation measures they have implemented, such as building floodwalls or elevating properties above sea level."

Other common types of business insurance may also be prone to AI bias. Business continuity insurance faces challenges when AI models—limited by data constraints—inaccurately assess a company's risks based on industry or location. For example, a manufacturing company in a rural setting might encounter higher premiums due to insufficient data that fails to consider its robust supply chain relationships, remote operability or contingency plans for power outages. Similarly, AI bias can impact directors and officers (D&O) insurance because AI models trained on industry-specific lawsuit data could inflate prices and restrict coverage for companies operating in sectors prone to litigation and insurance claims, overlooking these specific companies' clean legal records and key governance practices.

The historical data used to train AI systems can also be problematic, said Peter Wood, an entrepreneur and chief technology officer at tech recruitment firm Spectrum Search. Historical biases rooted in the data used in AI algorithms can adversely impact companies and lead to "skewed" risk assessments, especially in niche or emerging sectors where historical data may not accurately reflect current realities. "As AI systems learn from past data, they might assign undue risk to certain companies based on outdated or irrelevant criteria, leading to higher premiums and restrictive coverages," he explained.

Risk professionals need to ask for more details about how AI is used when underwriting policies and what checks and balances are employed to ensure the accuracy of results.

To counter AI bias concerns, Ryan Purdy, senior director and consulting actuary at tech and professional services firm Davies Group, said insurers need to understand the nature of any external data sources they intend to use for underwriting, including who provides the information in its root state, how it is updated and how often. "Data ages and can become less important to the assessment of risk or product suitability for a customer over time," he said.

Addressing AI Underwriting Concerns

Companies need to adopt proactive approaches when dealing with AI-driven insurance under-

writing. The key is to engage in transparent dialogue with insurers. "Companies should inquire about the nature of data sets used for training the AI models," Wood said. "It is essential to understand whether these datasets encompass a wide range of industries, including the latest trends and developments."

He added, "Companies should ask insurers about the mechanisms in place to identify and mitigate biases. This includes questioning whether the AI systems are regularly audited for fairness and accuracy. Additionally, they should inquire about the possibility of manual reviews

or overrides in cases where AI-driven decisions seem unjustly skewed."

Due to the potential for flawed outcomes, companies need to ask more questions about how risks evaluated through AI technologies are assessed and priced. While regulators may be keenly watching insurers for possible abuses regarding the treatment of consumers, "there are fewer safeguards for corporate insureds that are viewed as 'sophisticated purchasers,'" said Tom Davey, co-founder and director of litigation at finance and insurance consultancy Factor Risk Management. As such, there is a greater need for companies to raise questions and concerns themselves.

According to Jeremy Stevens, EMEA business unit director at insurance services provider Charles Taylor Group, companies need to ensure that their insurers can guarantee transparency in their AI decision-making processes. To do so, he said, "companies can ask for explanations on how these models arrive at decisions affecting premium pricing, underwriting and claims handling." Insurers, in turn, "should provide detailed documentation or reports that outline the factors and data inputs considered by AI models as these will help companies understand the rationale behind decisions," he said.

Companies should make sure that their insurers maintain comprehensive audit trails that trace the decision-making process of AI models to ensure full accountability. "Insurers must comply with industry standards and regulations that govern AI in insurance," Stevens said. "Companies can request information on how the insurer adheres to ethical AI practices and regulatory guidelines, so insurers must ensure their audit functions do not lag behind regulations."

Companies should also ask whether the insurer is continuously evaluating and monitoring the AI algorithm's performance, how the insurer arrives at specific decisions, and whether it regularly checks for biases, errors or changes in the data that might affect underwriting decisions. Other steps include checking that the insurer's AI-based underwriting system complies with various data laws such as the European Union's AI Act, the EU's General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA) and the U.S. Health Insurance Portability and Accountability Act (HIPAA), as well as various ethical standards. To better address these issues, companies can establish a collaborative relationship with their insurer. "Provide feedback on decisions and discuss how they align with your company's risk assessment," Stevens said.

It is also important to understand what kind of tech support insurers are getting if they use third-party AI tools. "How often their data is captured is important, but insurers should also work to understand how long it might be until the next update of the technology is available," Purdy said. "Are these future changes in data collection, data structures or technology versions going to force additional changes from the insurer side to keep making effective use of these technologies? Working to line up these providers' development timelines to the insurer's own timelines can alleviate substantial headaches in the future."

Data security is another area of concern. Experts warn that companies could be in danger of making key risk information publicly available if insurers use or share their data on AI systems—which often retain rights to the intellectual property of any inputted data—when training AI technologies to improve their underwriting. Companies need to actively protect their risk data by maintaining confidentiality, sharing it selectively, and enforcing contractual clauses for data protection, Wood said. They also need to vigilantly monitor the use of their data and check on what cybersecurity measures the insurer has in place to protect data from breaches or misuse.

"Companies should demand clarity on how their data will be used and ensure that their information is anonymized before being incorporated into larger datasets," Wood said. "This includes negotiating agreements that restrict the use of their data solely for underwriting purposes and not for training AI models. Insurers, for their part, must adhere to stringent data protection regulations and employ advanced encryption and access control mechanisms to prevent unauthorized data usage, too."

He added, "Furthermore, there should be transparency about data handling practices. Regular audits and compliance checks can help maintain trust and ensure that both parties adhere to the agreed-upon terms regarding data usage and privacy." R

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

SHUTTERSTOCK/FAMILY STOCK

RIMS-CRMP

RIMS-Certified Risk Management Professional

Get Certified

Start Your Application Today

Are you looking for a way to distinguish yourself and demonstrate your risk competence? Earn the RIMS-Certified Risk Management Professional (RIMS-CRMP) certification.

The RIMS-CRMP is the gold standard that you deserve: it is the only risk management credential that is competency-based and accredited by the ANSI National Accreditation Board.

Add the RIMS-CRMP to your professional profile to elevate your career. Join an elite group of risk professionals.

Learn more about the application process and exam prep workshops at **www.RIMS.org/Certification**

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

RIMS
the risk management society